AULA 02 – SEGURANÇA DA INFORMAÇÃO E TÓPICOS RELACIONADOS.

Olá pessoal,

Bom revê-los aqui para mais um encontro.

Nesta aula final vamos abordar o assunto **segurança da informação**. Todos prontos? Então vamos nessa ☺! Força aí, pessoal!

Prof^a^ Patrícia Lima Quintão
Instagram: patriciaquintao

Facebook: http://www.facebook.com/professorapatriciaquintao (Todo dia com novas dicas, desafios e muito mais, espero vocês por lá para **CURTIR** a página!)

Twitter: http://www.twitter.com/pquintao

Conteúdo desta Aula	**Página**

O que Significa Segurança?

É colocar tranca nas portas de sua casa? É ter as informações guardadas de forma suficientemente segura para que pessoas sem autorização não tenham acesso a elas? **Vamos nos preparar para que a próxima vítima não seja você ☺!!!**

A **segurança** é uma palavra que está presente em nosso cotidiano e **refere-se a um estado de proteção, em que estamos "livres" de perigos e incertezas!**

Segurança da informação é o processo de proteger a informação de diversos tipos de ameaças externas e internas para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

Em uma corporação, a segurança está ligada a tudo o que manipula direta ou indiretamente a informação (inclui-se aí também a própria informação e os usuários!!!), e que merece proteção.

Esses elementos são chamados de **ATIVOS**, e podem ser divididos em:

- tangíveis: informações impressas, móveis, hardware (Ex.:impressoras, *scanners*);
- intangíveis: marca de um produto, nome da empresa, confiabilidade de um órgão federal etc.;
- lógicos: informações armazenadas em uma rede, sistema ERP (sistema de gestão integrada), etc.;
- físicos: galpão, sistema de eletricidade, estação de trabalho, etc;
- humanos: funcionários.

Quanto maior for a organização maior será sua dependência com relação à informação, que pode estar armazenada de várias formas: impressa em papel, em meios digitais (discos, fitas, DVDs, disquetes, *pendrives,* etc.), na mente das pessoas, em imagens armazenadas em fotografias/filmes...

Soluções pontuais isoladas não resolvem toda a problemática associada à segurança da informação. **Segurança se faz em pedaços, porém todos eles integrados**, como se fossem uma corrente.

Segurança se faz protegendo todos os elos da corrente, ou seja, todos os ativos (físicos, tecnológicos e humanos) que compõem seu negócio. Afinal, o poder de proteção da corrente está diretamente associado ao elo mais fraco!

Princípios da Segurança da Informação

A segurança da informação busca proteger os **ativos** de uma empresa ou indivíduo com base na preservação de alguns princípios. Vamos ao estudo de cada um deles!!

Os quatro **princípios** considerados centrais ou principais, mais comumente cobrados em provas, são: a **C**onfidencialidade, a **I**ntegridade, a **D**isponibilidade e a **A**utenticidade (É possível encontrar a sigla **CIDA**, ou **DICA**, para fazer menção a estes princípios!).

Disponibilidade
Integridade
Confidencialidade
Autenticidade

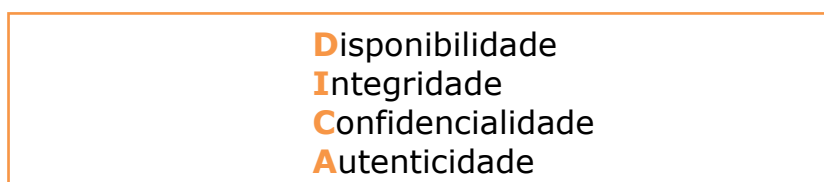



Figura. Mnemônico DICA

- **Confidencialidade (ou sigilo): é a garantia de que a informação não será conhecida por quem não deve**. O acesso às informações deve ser limitado, ou seja, **somente as pessoas explicitamente autorizadas podem acessá-las**. Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas sem a devida autorização para acessá-la.

  Exemplo: o número do seu cartão de crédito só poderá ser conhecido por você e pela loja em que é usado. Se esse número for descoberto por alguém mal intencionado, o prejuízo causado pela perda de confidencialidade poderá ser elevado, já que poderão se fazer passar por você para realizar compras pela Internet, proporcionando-lhe prejuízos financeiros e uma grande dor de cabeça!

- **Integridade:** destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais, indevidas ou acidentais. Em outras palavras, **é a garantia de que a informação que foi armazenada é a que será recuperada!!!**

A quebra de integridade pode ser considerada sob 2 aspectos:

1. alterações nos elementos que suportam a informação - são feitas **alterações na estrutura física e lógica em que uma informação está armazenada**. Por exemplo quando são alteradas as configurações de um sistema para ter acesso a informações restritas;
2. **alterações do conteúdo dos documentos**:
    - ex1.: imagine que alguém invada o *notebook* que está sendo utilizado para realizar a sua declaração do Imposto de Renda deste ano, e, momentos antes de você enviá-la para a Receita Federal a mesma é alterada sem o seu consentimento! Neste caso, a informação não será transmitida da maneira adequada, o que <u>quebra</u> o princípio da integridade;
    - ex2: alteração de *sites* por *hackers* (*vide* a figura seguinte, retirada de http://www.fayerwayer.com.br/2013/06/site-do-governo-brasileiro-e-hackeado/). Acesso em jul. 2013.

Figura. Portal Brasil (www.brasil.gov.br), página oficial do governo brasileiro na Internet, que teve seu conteúdo alterado indevidamente em jun. 2013.

- **<u>D</u>isponibilidade**: é a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo. Em outras palavras, **<u>é a garantia que a informação sempre poderá ser acessada</u>!!!**

  Como exemplo, há quebra do princípio da disponibilidade quando você decidir enviar a sua declaração do Imposto de Renda pela Internet, no último dia possível, e o *site* da Receita Federal estiver indisponível.

- **<u>A</u>utenticidade (**considerada por alguns autores como **autenticação):** é a capacidade de garantir a **identidade de uma pessoa (física ou jurídica) que acessa as informações do sistema ou de um servidor**

(computador) com quem se estabelece uma transação (de comunicação, como um *e-mail*, ou comercial, como uma venda *on-line*). **É por meio da autenticação que se confirma a identidade da pessoa ou entidade que presta ou acessa as informações!** Recursos como senhas (que, teoricamente, só o usuário conhece), biometria, assinatura digital e certificação digital são usados para essa finalidade.

O que queremos sob a ótica de segurança?

Desejamos entregar a informação CORRETA, para a pessoa CERTA, no momento CORRETO, confirmando a IDENTIDADE da pessoa ou entidade que presta ou acessa as informações!!! Entenderam??

Eis a essência da aplicação dos quatro princípios acima destacados. Ainda, cabe destacar que **a perda de pelo menos um desses princípios já irá ocasionar impactos ao negócio** (aí surgem os **incidentes de segurança**!!)

Quando falamos em segurança da informação, estamos nos referindo a **salvaguardas para manter a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente**!

Fique Atento!

Incidente de segurança da informação: é indicado por um **simples ou por uma série de eventos de segurança da informação indesejados ou inesperados**, que tenham uma grande probabilidade de **comprometer** as operações do negócio e ameaçar a segurança. Exemplos: invasão digital; violação de padrões de segurança de informação.

Outros princípios podem ainda ser também levados em consideração, como por exemplo:

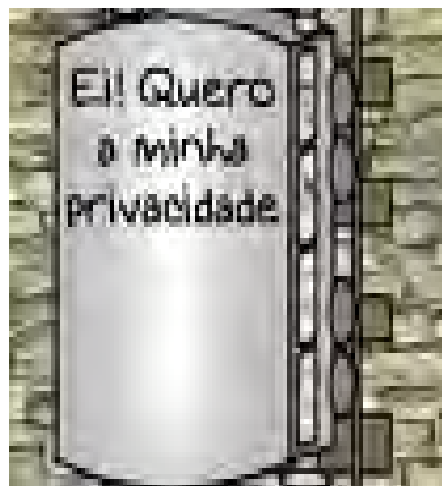
- **Confiabilidade:** pode ser caracterizada como a condição em que um sistema de informação presta seus serviços de forma eficaz e eficiente, ou melhor, um sistema de informação irá "desempenhar o papel que foi proposto para si".

Fique Atento!

Confiabilidade: visa garantir que um sistema vai se comportar (vai realizar seu serviço) segundo o esperado e projetado ("**ser confiável**", "**fazer bem seu papel**").

- **Não-repúdio (irretratabilidade):** é a **garantia de que um agente não consiga negar (dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação**. Tal garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver autenticidade e integridade (ou seja, quando for possível determinar quem mandou a mensagem e garantir que a mesma não foi alterada).
- **Legalidade: aderência do sistema à legislação**.
- **Auditoria**: é a **possibilidade de rastrear o histórico dos eventos de um sistema** para determinar quando e onde ocorreu uma violação de segurança, bem como identificar os envolvidos nesse processo.
- **Privacidade:** diz respeito ao direito fundamental de cada indivíduo de decidir quem deve ter acesso aos seus dados pessoais.

  A privacidade é a capacidade de um sistema manter incógnito um usuário (capacidade de um usuário realizar operações em um sistema sem que seja identificado), **<u>impossibilitando a ligação direta da identidade do usuário com as ações por este realizadas</u>**. Privacidade é uma característica de segurança requerida, por exemplo, em eleições secretas.

  Uma informação privada deve ser vista, lida ou alterada somente pelo seu dono. Esse princípio difere da confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada.

Vulnerabilidades de Segurança

Vulnerabilidade é uma **fragilidade** que poderia ser explorada por uma ameaça para concretizar um ataque.

Outro conceito bastante comum para o termo:

Vulnerabilidade é uma evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio, aumentando a probabilidade de sucesso pela investida de uma ameaça.

Ainda, trata-se de **falha no projeto, implementação ou configuração de software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador**.

O conhecimento do maior número de vulnerabilidades possíveis permite à equipe de segurança tomar **medidas para proteção**, evitando assim ataques e consequentemente perda de dados.

Não há uma receita ou lista padrão de vulnerabilidades. Esta deve ser levantada junto a cada organização ou ambiente. Sempre se deve ter em mente o que precisa ser protegido e de quem precisa ser protegido de acordo com as ameaças existentes. Podemos citar, como exemplo inicial, uma análise de ambiente em uma sala de servidores de conectividade e Internet com a seguinte descrição: a sala dos servidores não possui controle de acesso físico!! Eis a vulnerabilidade detectada nesse ambiente.

Outros exemplos de vulnerabilidades:

• ambientes com informações sigilosas com acesso não controlado;	• hardware sem o devido acondicionamento e proteção;
• *software* mal desenvolvido;	• falta de atualização de *software* e hardware;
• falta de mecanismos de monitoramento e controle (auditoria);	• ausência de pessoal capacitado para a segurança;
• inexistência de políticas de segurança;	• instalações prediais fora do padrão;
• ausência de recursos para combate a incêndios, etc.	

Golpes na Internet

A seguir apresentamos alguns dos principais golpes aplicados na Internet, comumente cobrados em provas:

- ***Phishing*** (também conhecido como ***Phishing scam,*** ou apenas ***scam***) **Importante!!!**

  É um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente.

  O golpe de phishing é realizado por uma pessoa mal-intencionada através da criação de um website falso e/ou do envio de uma mensagem eletrônica falsa, geralmente um e-mail ou recado através de scrapbooks como no sítio Orkut, entre outros exemplos.

  Utilizando de pretextos falsos, tenta enganar o receptor da mensagem e induzi-lo a fornecer informações sensíveis (números de cartões de crédito, senhas, dados de contas bancárias, entre outras).

  As duas figuras seguintes apresentam "iscas" (*e-mails*) utilizadas em golpes de *phishing*, uma envolvendo o Banco de Brasil e a outra o Serasa.

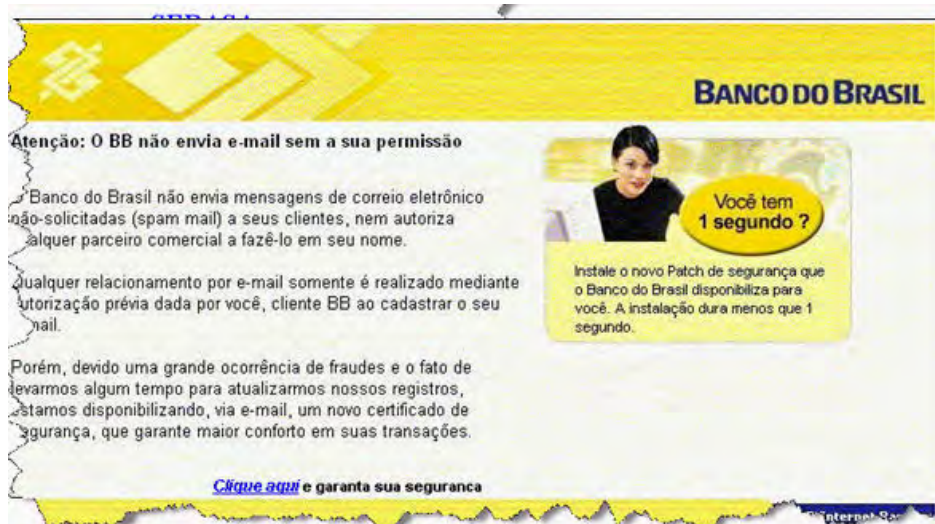



Figura. Isca de *Phishing* Relacionada ao Banco do Brasil

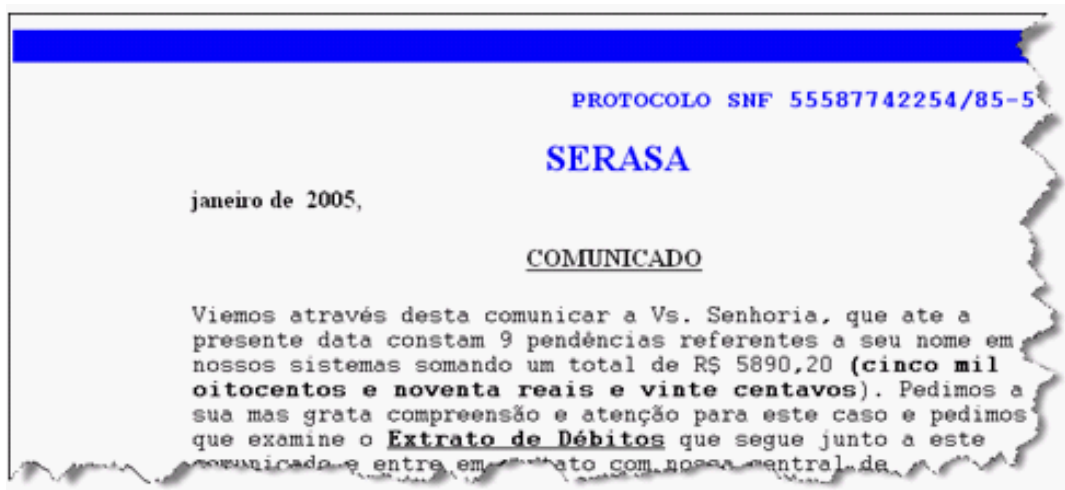



Figura. Isca de Phishing Relacionada ao SERASA

A palavra phishing (de fishing) vem de uma analogia criada pelos fraudadores, em que "iscas" (e-mails) são usadas para "pescar" informações sensíveis (senhas e dados financeiros, por exemplo) de usuários da Internet.

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

- **Pharming**

O Pharming é uma técnica que **utiliza o sequestro ou a "contaminação" do servidor DNS** (*Domain Name Server*) **para levar os usuários a um site falso, alterando o DNS do site de destino.** O sistema também pode redirecionar os usuários para sites autênticos através de proxies controlados, que podem ser usados para monitorar e interceptar a digitação.

Os sites falsificados coletam números de cartões de crédito, nomes de contas, senhas e números de documentos. Isso é feito através da exibição de um pop-up para roubar a informação antes de levar o usuário ao site real. O programa mal-intencionado usa um certificado auto-assinado para fingir a autenticação e induzir o usuário a acreditar nele o bastante para inserir seus dados pessoais no site falsificado. Outra forma de enganar o usuário é sobrepor a barra de endereço e status de navegador para induzi-lo a pensar que está no site legítimo e inserir suas informações.

Nesse contexto, programas criminosos podem ser instalados nos PCs dos consumidores para roubar diretamente as suas informações. Na maioria dos casos, o usuário não sabe que está infectado, percebendo apenas uma ligeira redução na velocidade do computador ou falhas de funcionamento atribuídas a vulnerabilidades normais de software.

Ataques na Internet

Rumo aos principais!

- **Engenharia Social**

  É o método de se obter dados importantes de pessoas através da velha "**lábia**". **A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Guarde isso!!!**

  Em redes corporativas que são alvos mais apetitosos para invasores, o perigo é ainda maior e pode estar até sentado ao seu lado. Um colega poderia tentar obter sua senha de acesso mesmo tendo uma própria, pois uma sabotagem feita com sua senha parece bem mais interessante do que com a senha do próprio autor.

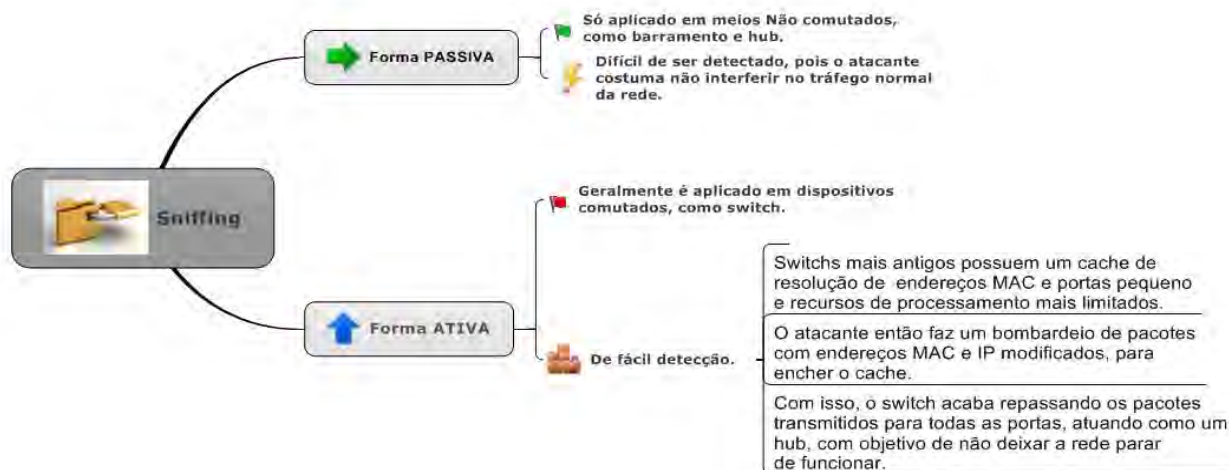
- ***Sniffing***

  Processo de captura das informações da rede por meio de um software de escuta de rede *(conhecido como sniffer, farejador ou ainda capturador de pacote)*, capaz de interpretar as informações transmitidas no meio físico.

Sniffers *(farejadores* ou ainda capturadores de pacotes*):* por padrão, os computadores (pertencentes à mesma rede) escutam e respondem somente pacotes endereçados a eles. Entretanto, é possível utilizar um software que coloca a interface num estado chamado de ***modo promíscuo***.

Nessa condição o computador pode monitorar e capturar os dados trafegados através da rede, não importando o seu destino legítimo.

Os programas responsáveis por capturar os pacotes de rede são chamados *Sniffers, Farejadores ou ainda Capturadores de Pacote*. Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados. Dessa maneira um sniffer atua na rede farejando pacotes na tentativa de encontrar certas informações, como nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada.

A dificuldade no uso de um *sniffer* é que o atacante precisa instalar o programa em algum ponto estratégico da rede, como entre duas máquinas, (com o tráfego entre elas passando pela máquina com o farejador) ou em uma rede local com a interface de rede em modo promíscuo.

- ***Denial of Service* (DoS)**

Os **ataques de negação de serviço** (***denial of service* - DoS**) consistem em impedir o funcionamento de uma máquina ou de um serviço específico. No caso de ataques a redes, geralmente ocorre que os usuários legítimos de uma rede não consigam mais acessar seus recursos.

O DoS acontece quando um atacante envia vários pacotes ou requisições de serviço de uma vez, com objetivo de sobrecarregar um servidor e, como consequência, impedir o fornecimento de um serviço para os demais usuários, causando prejuízos.

Fique Atento!

No DoS o atacante utiliza um computador para tirar de operação um serviço ou computador(es) conectado(s) à Internet!!.

Como exemplo deste tipo de ataque tem-se o seguinte contexto: gerar uma sobrecarga no processamento de um computador, de modo que o usuário não consiga utilizá-lo; gerar um grande tráfego de dados para uma rede, ocasionando a indisponibilidade dela; indisponibilizar serviços importantes de um provedor, impossibilitando o acesso de seus usuários.

Cabe ressaltar que se uma rede ou computador sofrer um DoS, isto não significa que houve uma invasão, pois o objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadi-los.

CAIU EM PROVA (Polícia Federal)

Um dos mais conhecidos ataques a um computador conectado a uma rede é o de negação de serviço (DoS – *Denial Of Service*), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.

- ***Distributed Denial of Service* (DDoS)** -> São os ataques coordenados!

Em dispositivos com grande capacidade de processamento, normalmente, é necessária uma enorme quantidade de requisições para que o ataque seja eficaz. Para isso, o atacante faz o uso de uma *botnet* (rede de computadores zumbis sob comando do atacante) para bombardear o servidor com requisições, fazendo com que o ataque seja feito de forma distribuída (*Distributed Denial of Service* – DDoS).

Fique Atento!

No DDoS - ataque de negação de serviço distribuído-, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

- **Ataques de senhas**

  A utilização de senhas seguras é um dos pontos fundamentais para uma estratégia efetiva de segurança, no entanto, muitos usuários priorizam a conveniência ao invés da segurança e utilizam senhas fáceis de serem descobertas e inseguras.

  As duas principais **técnicas de ataque a senhas** são:

  - **Ataque de Dicionário**: nesse tipo de ataque são utilizadas combinações de palavras, frases, letras, números, símbolos, ou qualquer outro tipo de combinação geralmente que possa ser utilizada na criação das senhas pelos usuários. Os programas responsáveis por realizar essa tarefa trabalham com diversas permutações e combinações sobre essas palavras. Quando alguma dessas combinações se referir à senha, ela é considerada como quebrada (***Cracked***).

    Geralmente as senhas estão armazenadas criptografadas utilizando um sistema de criptografia HASH. Dessa maneira os programas utilizam o mesmo algoritmo de criptografia para comparar as combinações com as senhas armazenadas. Em outras palavras, eles adotam a mesma configuração de criptografia das senhas, e então criptografam as palavras do dicionário e comparam com senha.

  - **Força-Bruta**: enquanto as listas de palavras, ou dicionários, dão ênfase na velocidade, o segundo método de quebra de senhas se baseia simplesmente na repetição. Força-Bruta é uma forma de se descobrir senhas que compara cada combinação e permutação possível de caracteres até achar a senha. Este é um método muito poderoso para descoberta de senhas, no entanto é extremamente lento porque cada combinação consecutiva de caracteres é comparada. Ex: aaa, aab, aac ..... aaA, aaB, aaC... aa0, aa1, aa2, aa3... aba, aca, ada...

- ***Ping of Death***

  Ele **consiste em enviar um pacote IP com tamanho maior que o máximo permitido (65.535 bytes) para a máquina atacada**. O pacote é enviado na forma de fragmentos (porque nenhuma rede permite o tráfego de pacotes deste tamanho), e quando a máquina destino tenta montar estes fragmentos, inúmeras situações podem ocorrer: a maioria trava, algumas reinicializam, outras exibem mensagens no console, etc.

- ***Dumpster diving ou trashing***

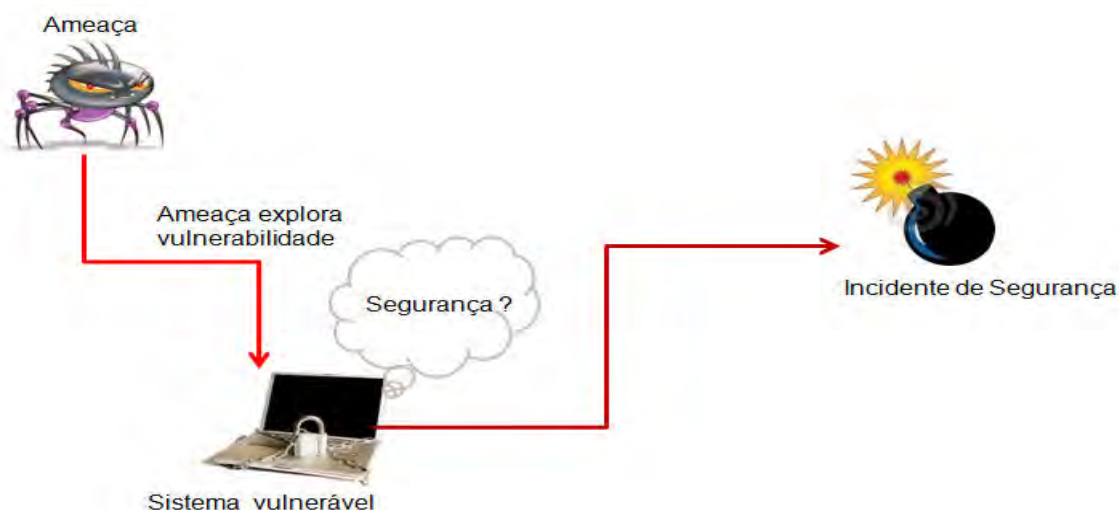
  É a atividade na qual **o lixo é verificado em busca de informações sobre a organização ou a rede da vítima**, como nomes de contas e

senhas, informações pessoais e confidenciais. Muitos dados sigilosos podem ser obtidos dessa maneira.

- **Esteganografia**: é a técnica de esconder um arquivo dentro de outro arquivo, podendo ser uma imagem, documento de texto, planilha eletrônica etc., só que utilizando criptografia. Ao esconder um arquivo em uma imagem, por exemplo, ao enviá-la para o destinatário desejado, você tem que se assegurar que quem receber a imagem deverá conhecer o método de exibição e a senha utilizada na proteção deste arquivo.

Figura 1 Esteganografia

Ameaças à Segurança

Ameaça é algo que possa provocar **danos** à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada **vulnerabilidade**.

Em outras palavras, uma **AMEAÇA é tudo aquilo que pode comprometer a segurança de um sistema, podendo ser acidental** (falha de *hardware*, erros de programação, desastres naturais, erros do usuário, *bugs* de *software*, uma ameaça secreta enviada a um endereço incorreto, etc.) **ou deliberada** (roubo, espionagem, fraude, sabotagem, invasão de *hackers*, entre outros).

Ameaça pode ser uma pessoa, uma coisa, um evento ou uma ideia capaz de causar dano a um recurso, em termos de confidencialidade, integridade, disponibilidade *etc*. Como exemplos de ameaça podemos destacar: concorrente, cracker, erro humano (deleção de arquivos digitais acidentalmente etc.), acidentes naturais (inundação etc.), funcionário insatisfeito, técnicas (engenharia social, etc.), ferramentas de software (sniffer, cavalo de troia, etc.).

Basicamente existem dois tipos de ameaças: internas e externas.

- **Ameaças externas**: tentativas de ataque e desvio de informações vindas de fora da empresa, normalmente realizadas por pessoas com a intenção de prejudicar a empresa ou para utilizar seus recursos para invadir outras empresas.
- **Ameaças internas**: estão presentes, independentemente das empresas estarem ou não conectadas à Internet. Podem causar desde incidentes leves até os mais graves, como a inatividade das operações da empresa.

Resumindo, temos que...

Os ATIVOS são os elementos que sustentam a operação do negócio e estes sempre trarão consigo VULNERABILIDADES que, por sua vez, submetem os ativos a AMEAÇAS.

Vírus, Worms e outras Pragas virtuais – Códigos Maliciosos que são AMEAÇAS à Segurança da Informação!!

Você sabe o significado de malware?

Malware (combinação de ***malicious software*** – ***programa malicioso***)!

O termo *Malware* é usado para todo e quaisquer *softwares* maliciosos, programados com o intuito de prejudicar os sistemas de informação, alterar o funcionamento de programas, roubar informações, causar lentidões de redes computacionais, dentre outros.

Resumindo, ***malwares*** **são programas que executam deliberadamente ações mal-intencionadas em um computador**!!

Certbr (2012) destaca algumas das diversas maneiras como os códigos maliciosos (malwares) podem infectar ou comprometer um computador. São elas:

- por meio da exploração de vulnerabilidades (falhas de segurança) existentes nos programas instalados;

- por meio da auto-execução de mídias removíveis infectadas, como pen-drives;
- pelo acesso a páginas da Web maliciosas, com a utilização de navegadores vulneráveis;
- por meio da ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Na categoria de malwares são incluídos os vírus de computador, Worms, entre outras "beldades" do mundo da informática, como:

-vírus,

-*worms*,

-*bots*,

-cavalos de troia (trojans),

-*spyware*,

-*keylogger*,

-*screenlogger*,

-ransomwares,

-*Backdoors*,

-Rootkits, *etc*.

- **Vírus**

São pequenos códigos de programação maliciosos que se "agregam" a arquivos e são transmitidos com eles. Em outras palavras, tecnicamente, um vírus é um programa (ou parte de um programa) que se anexa a um arquivo de programa qualquer (como se o estivesse "parasitando") e depois disso procura fazer cópias de si mesmo em outros arquivos semelhantes.

Quando o arquivo é aberto na memória RAM, o vírus também é, e, a partir daí se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

O vírus **depende da execução do programa ou arquivo hospedeiro** para que possa se tornar ativo e dar continuidade ao processo de infecção. Alguns vírus são inofensivos, outros, porém, podem danificar um sistema operacional e os programas de um computador.

A seguir destacamos alguns arquivos que podem ser **portadores de vírus de computador**:

- arquivos executáveis: com extensão .exe ou .com;
- arquivos de scripts (outra forma de executável): extensão .vbs;
- atalhos: extensão .lnk ou .pif;
- proteção de tela (animações que aparecem automaticamente quando o computador está ocioso): extensão .scr;
- documentos do MS-Office: como os arquivos do Word (extensão .doc ou .dot), arquivos do Excel (.xls e .xlt), apresentações do Powerpoint (.ppt e .pps), bancos de dados do Access (.mdb).
- arquivos multimídia do Windows Media Player: músicas com extensão .WMA, vídeos com extensão .WMV, dentre outros.

Dentre os **principais tipos de vírus** conhecidos merecem destaque:

Vírus Polimórficos	**Alteram seu formato ("mudam de forma") constantemente.** A cada nova infecção, esses vírus geram uma nova sequência de bytes em seu código, para que o antivírus se confunda na hora de executar a varredura e não reconheça o invasor.
Vírus Oligomórfico	Usa a criptografia para se defender sendo capaz de alterar também a rotina de criptografia em um número de vezes pequeno. Um vírus que possui duas rotinas de decriptografia é então classificado como oligomórfico (Luppi, 2006).
Vírus de Macro	Vírus que **infectam documentos que contém macros.** ***Macro:* conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar tarefas repetitivas.** Um exemplo seria, em um editor de textos, definir uma macro que contenha a sequência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons de cinza. Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros. Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador. Existem alguns aplicativos que possuem arquivos base (**modelos**) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus

	de macro, toda vez que o aplicativo for executado, o vírus também será. **Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access são os mais suscetíveis a este tipo de vírus.** Arquivos nos formatos RTF, PDF e PostScript são menos suscetíveis, mas isso não significa que não possam conter vírus. Normal.dot Modelo do Microsoft Word 14 KB Normal.dot–Principal alvo de vírus de macro p/Word
Vírus de Boot	**Infectam o setor de boot** (ou MBR – Master Boot Record – Registro Mestre de Inicialização) **dos discos rígidos.** Obs.: o Setor de Boot do disco rígido é a primeira parte do disco rígido que é lida quando o computador é ligado. Essa área é lida pelo BIOS (programa responsável por "acordar" o computador) a fim de que seja encontrado o Sistema Operacional (o programa que vai controlar o computador durante seu uso).
Vírus de Programa	**Infectam arquivos de programa** (de inúmeras extensões, como .exe, .com,.vbs, .pif.
Vírus *Stealth*	**Programado para se esconder e enganar o antivírus durante uma varredura deste programa**. Tem a capacidade de se remover da memória temporariamente para evitar que antivírus o detecte.
Vírus de *Script*	**Propagam-se por meio de *scripts***, nome que designa uma sequência de comandos previamente estabelecidos e que são executados automaticamente em um sistema, sem necessidade de intervenção do usuário. Dois tipos de *scripts* muito usados são os projetados com as linguagens Javascript (JS) e Visual Basic Script (VBS). Tanto um quanto o outro podem ser inseridos em páginas Web e interpretados por navegadores como Internet Explorer e outros. Os arquivos Javascript tornaram-se tão comuns na Internet que é difícil encontrar algum *site* atual que não os utilize. Assim como as macros, os *scripts* não são necessariamente maléficos. Na maioria das vezes executam tarefas úteis, que facilitam a vida dos usuários – prova disso é que se a execução dos *scripts* for desativada nos navegadores, a maioria dos *sites* passará a ser apresentada de forma incompleta ou incorreta.
Vírus de Telefone	Propaga de telefone para telefone através da tecnologia *bluetooth* ou da tecnologia MMS (*Multimedia Message*

Celular	*Service*). O serviço MMS é usado para enviar mensagens multimídia, isto é, que contêm não só texto, mas também sons e imagens, como vídeos, fotos e animações. A infecção ocorre da seguinte forma: o usuário recebe uma mensagem que diz que seu telefone está prestes a receber um arquivo e permite que o arquivo infectado seja recebido, instalado e executado em seu aparelho; o vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente. Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no telefone celular, mas podem ser especificamente projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho. Depois de infectar um telefone celular, o vírus pode realizar diversas atividades, tais como: • destruir/sobrescrever arquivos; • remover contatos da agenda; • efetuar ligações telefônicas; • o aparelho fica desconfigurado e tentando se conectar via Bluetooth com outros celulares; • a bateria do celular dura menos do que o previsto pelo fabricante, mesmo quando você não fica horas pendurado nele; • emitir algumas mensagens multimídia esquisitas; • tentar se propagar para outros telefones.

- ***Worms* (Vermes)**

Programas parecidos com vírus, mas que na verdade **são capazes de se propagarem <u>automaticamente</u> através de rede**s, enviando cópias de si mesmo de computador para computador (observe que os *worms* apenas se copiam, **<u>não</u> infectam outros arquivos, eles mesmos são os arquivos** !!). Além disso, geralmente

utilizam as redes de comunicação para infectar outros computadores (via *e-mails*, Web, FTP, redes das empresas etc.).

Diferentemente do vírus, **o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.** *Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.*

Os Worms podem se espalhar de diversas maneiras, mas a propagação via rede é a mais comum. Sua característica marcante é a replicação (cópia funcional de si mesmo) e infecção de outros computadores **SEM intervenção humana** e SEM **necessidade de um programa hospedeiro**. **(Atenção)**

Worms são notadamente responsáveis por consumir muitos recursos. **Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.** Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Difíceis de serem detectados, muitas vezes os worms realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. Embora alguns programas antivírus permitam detectar a presença de Worms e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

- ***Bots* ("Robôs")**

De modo similar ao *worm*, é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalado em um computador.

Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente. Os *bots* esperam por comandos de um *hacker*, podendo manipular os sistemas infectados, sem o conhecimento do usuário.

Segundo CertBr(2012) a comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Nesse ponto, cabe destacar um termo que já foi cobrado várias vezes em prova pela banca!! Trata-se do significado do termo ***botnet***, junção da contração das palavras *robot* (*bot*) e *network* (*net*). Uma rede infectada por *bots* é denominada de ***botnet*** (também conhecida como **rede zumbi**), sendo composta geralmente por milhares desses elementos

maliciosos que ficam residentes nas máquinas, aguardando o comando de um invasor.

Quanto mais zumbis (zombie computers) participarem da botnet mais potente ela será. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para coletar informações de um grande número de computadores, aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço etc. (CERT.br, 2012).

O esquema simplificado apresentado a seguir destaca o funcionamento básico de uma botnet (CERT.br, 2012):

- o atacante propaga um tipo específico de bot com a intenção de infectar e conseguir a maior quantidade possível de máquinas zumbis;
- essas máquinas zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
- quando o controlador deseja que uma ação seja realizada, ele envia às máquinas zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;
- as máquinas zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
- quando a ação é encerrada, as máquinas zumbis voltam a ficar à espera dos próximos comandos a serem executados.

- ***Trojan Horse* (Cavalo de Troia)**

É um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc., e que, quando executado (com a sua autorização!), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido.

Por definição, o Cavalo de Troia distingue-se de um vírus ou de um *worm* por **não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente**.

O *trojans* ficaram famosos na Internet pela facilidade de uso, e por permitirem a qualquer pessoa possuir o controle de um outro computador apenas com o envio de um arquivo.

Os *trojans* atuais são divididos em duas partes, que são: o servidor e o cliente. Normalmente, o **servidor** encontra-se oculto em algum outro arquivo e, no momento em que o arquivo é executado, o servidor se instala

e se oculta no computador da vítima. Nesse momento, o computador já pode ser acessado pelo **cliente**, que enviará informações para o servidor executar certas operações no computador da vítima.

O Cavalo de Troia não é um vírus, pois não se duplica e não se dissemina como os vírus. Na maioria das vezes, ele irá instalar programas para possibilitar que um invasor tenha controle total sobre um computador.

Estes programas podem permitir que o invasor:

- veja e copie ou destrua todos os arquivos armazenados no computador;
- instalação de *keyloggers* ou *screenloggers* (descubra todas as senhas digitadas pelo usuário);
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador;
- formate o disco rígido do computador, etc.

Exemplos comuns de Cavalos de Troia são programas que você recebe ou obtém de algum site e que parecem ser apenas cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, entre outros. Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar *backdoors*, alterar informações, apagar arquivos ou formatar o disco rígido.

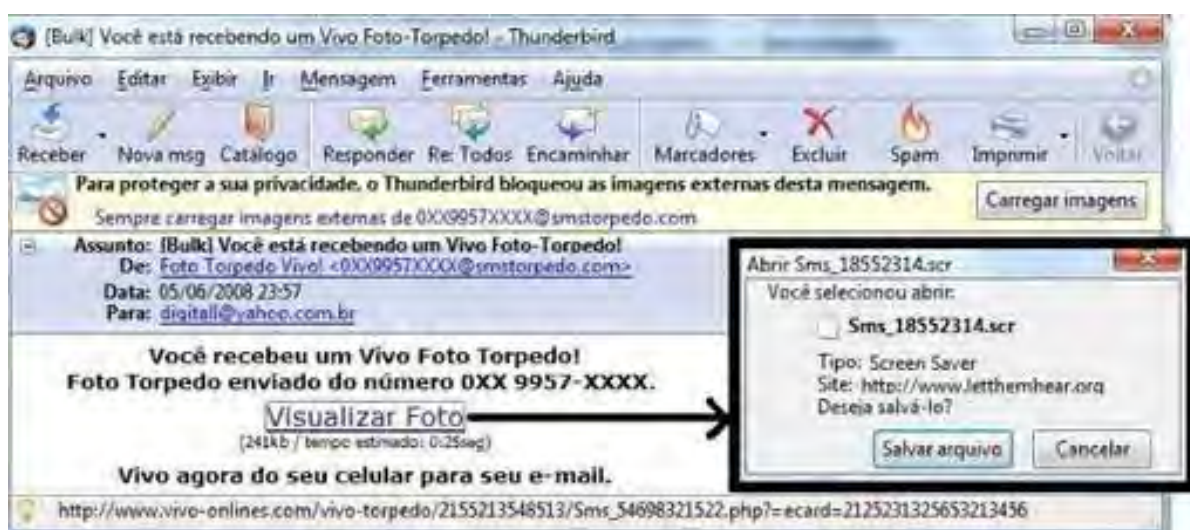



Figura. Um spam contendo um Cavalo de Troia. O usuário será infectado se clicar no link e executar o anexo.

- ***Spyware***

Trata-se de um **programa espião (*spy* em inglês = espião),** que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Vamos à diferença entre seu uso:

- **Legítimo**: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
- **Malicioso**: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:

Keylogger ***(Copia as teclas digitadas!)***

Um tipo de *malware* que é **capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador**. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito. Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou Internet Banking. Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

Screenloggers ***(Copia as telas acessadas!)***

As instituições financeiras desenvolveram os teclados virtuais para evitar que os keyloggers pudessem capturar informações sensíveis de usuários. Então, foram desenvolvidas formas mais avançadas de keyloggers, também conhecidas como **screenloggers** capazes de: armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

Normalmente, o keylogger vem como parte de um programa spyware ou cavalo de troia. Desta forma, é necessário que este programa seja executado para que o keylogger se instale em um computador. Geralmente, tais programas vêm anexados a e-mails ou estão disponíveis em sites na Internet. Existem ainda programas leitores de e-mails que podem estar

configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que qualquer arquivo anexado seja executado.

***Adware* (*Advertising software*)**

Projetado especificamente para apresentar propagandas. Este tipo de programa geralmente não prejudica o computador. O *adware* apresenta anúncios, cria ícones ou modifica itens do sistema operacional com o intuito de exibir alguma propaganda. Um *adware* malicioso pode abrir uma janela do navegador apontando para páginas de cassinos, vendas de remédios, páginas pornográficas, etc. Um exemplo do uso legítimo de *adwares* pode ser observado no programa de troca instantânea de mensagens MSN Messenger.

- ***Ransomwares*** **(Pede resgate!)**

São softwares maliciosos que, ao infectarem um computador, *criptografam todo ou parte do conteúdo do disco rígido*. Os responsáveis pelo software exigem da vítima, um pagamento pelo "resgate" dos dados.

Fique Atento!

Em 2012, a McAfee "observou o aumento do número de **ameaças móveis**, com a expansão do **ransomware (sequestro de equipamentos) para dispositivos móveis**. O desenvolvimento e a distribuição de tecnologias de ransomware sofisticadas, que impedem o uso de telefones ou tablets e ameaçam mantê-los assim até que um resgate seja pago, são uma **tendência considerável em 2013".** "Como os atacantes sequestram a capacidade de o usuário acessar seus dados, as vítimas terão as opções de perder suas informações ou **pagar resgate** para recuperar o acesso". Fonte: http://adrenaline.uol.com.br/seguranca/noticias/15160/mcafee-preve-as-principais-ameacas-para-2013.html

- **Backdoors (Abre portas)**

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado. A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de **backdoor**.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão

alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de troia. Programas de administração remota, como BackOrifice, NetBus, Sub-Seven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

- **Rootkit**

Tipo de *malware* cuja principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus. Isto é possível por que esta aplicação tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado.

O invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, merecem destaque:

- programas para esconder atividades e informações deixadas pelo invasor, tais como arquivos, diretórios, processos etc.;
- *backdoors*, para assegurar o acesso futuro do invasor ao computador comprometido;
- programas para remoção de evidências em arquivos de *logs*;
- *sniffers*, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- *scanners*, para mapear potenciais vulnerabilidades em outros computadores.

Spams

São mensagens de correio eletrônico não autorizadas ou não solicitadas, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

O *spam* não é propriamente uma ameaça à segurança, mas é um **portador comum delas**. São *spams*, por exemplo, os e-mails falsos que recebemos como sendo de órgãos como Receita Federal ou Tribunal Superior Eleitoral. Nesse caso, os *spams* costumam induzir o usuário a instalar um dos *malwares* que vimos anteriormente.

Os spammers (indivíduos que enviam spams) utilizam diversas técnicas para coletar os endereços de e-mail, desde a compra de bancos de dados até a produção de suas próprias listas, geradas a partir de (CERTBR, 2013):

- **Ataques de dicionário**: consistem em formar endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.
- **Códigos maliciosos**: muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de e-mail que, posteriormente, são repassados para os spammers.
- **Harvesting**: consiste em coletar endereços de e-mail por meio de varreduras em páginas Web e arquivos de listas de discussão, entre outros.

Cookies

São pequenos arquivos que são instalados em seu computador durante a navegação, permitindo que os sites (servidores) obtenham determinadas informações. É isto que permite que alguns sites o cumprimentem pelo nome, saibam quantas vezes você o visitou, etc.

A seguir destacamos alguns dos riscos relacionados ao uso de cookies (CERTBR,2013):

- **informações coletadas pelos cookies** podem ser indevidamente compartilhadas com outros sites e afetar a sua privacidade;
- **exploração de vulnerabilidades existentes no computador.** Ao acessar uma página da Web o seu navegador disponibiliza uma serie de informações sobre a máquina como hardware, sistema operacional e programas instalados. Os cookies podem ser utilizados para manter referências contendo estas informações e usá-las para explorar possíveis vulnerabilidades existentes em seu computador;
- **autenticação automática**: quando utilizamos as opções como "Lembre-se de mim" e "Continuar conectado" nos ˜sites visitados, os cookies guardam essas informações para autenticações futuras. Em caso de uma máquina contaminada, essa prática pode permitir que outras pessoas se autentiquem como você;
- **coleta de informações pessoais**: dados preenchidos em formulários Web também podem ser gravados em cookies, coletados por atacantes ou códigos maliciosos e indevidamente acessados, caso não estejam criptografados;
- **coleta de hábitos de navegação**: quando você acessa diferentes sites onde são usados cookies de terceiros, pertencentes a uma mesma empresa de publicidade, é possível a esta empresa determinar seus hábitos de navegação e, assim, comprometer a sua privacidade.

Códigos móveis

Utilizados por desenvolvedores para incorporar maior funcionalidade e melhorar a aparência das páginas *Web*. Podem representar riscos quando mal implementados ou usados por pessoas mal-intencionadas.

Exemplos:

- **Programas e *applets Java*:** podem conter falhas de implementação e permitir que um programa Java hostil viole a segurança do computador;

- ***JavaScripts*:** podem ser usados para causar violações de segurança em computadores;
- **Componentes (ou controles) *ActiveX*:** Certbr (2013) destaca que o navegador *Web*, pelo esquema de certificados digitais, verifica a procedência de um componente *ActiveX* antes de recebê-lo. Ao aceitar o certificado, o componente é executado e pode efetuar qualquer tipo de ação, desde enviar um arquivo pela Internet até instalar programas (que podem ter fins maliciosos) em seu computador.

Janelas de *pop-up*

Aparecem automaticamente e sem permissão do usuário, sobrepondo a janela do navegador *Web*, após o acesso a um determinado *site*.

Certbr (2013) destaca alguns riscos que podem ser ocasionados nesse contexto:

- apresentar mensagens indesejadas, contendo propagandas ou conteúdo impróprio;
- apresentar *links*, que podem redirecionar a navegação para uma página falsa ou induzi-lo a instalar códigos maliciosos.

Plug-ins, complementos e extensões

São programas geralmente desenvolvidos por terceiros e que você pode instalar em seu navegador *Web* ou leitor de *e-mails* para prover funcionalidades extras.

Apesar de grande parte desses programas serem confiáveis, há a chance de existir programas especificamente criados para executar atividades maliciosas ou que, devido a erros de implementação, possam executar ações danosas em seu computador (Certbr,2013).

Links patrocinados

O Link patrocinado é um formato de anúncio publicitário pago, oferecido por diversas ferramentas de busca como: Google, Yahoo, Bing. Um **anunciante** que queira fazer propaganda de um produto

ou site paga para o site de busca apresentar o link em destaque (vide figura seguinte) quando palavras específicas são pesquisadas. <u>Quando se clica em um link patrocinado, o site de busca recebe do anunciante um valor previamente combinado</u>.

Segundo Certbr (2013) o anunciante geralmente possui uma página Web - com acesso via conta de usuário e senha - para poder interagir com o site de busca, alterar configurações, verificar acessos e fazer pagamentos. Este tipo de conta é bastante visado por atacantes, com o intuito de criar redirecionamentos para páginas de phishing ou contendo códigos maliciosos e representa o principal risco relacionado a links patrocinados.

Banners de propaganda

Caso você tenha uma página Web, é possível disponibilizar um espaço nela para que o serviço de publicidade apresente banners de seus clientes. Quanto mais a sua página é acessada e quanto mais cliques são feitos nos banners por intermédio dela, mais você pode vir a ser remunerado.

Um golpe decorrente desse ambiente é o **malvertising** (junção de "**malicious**" (malicioso) e "**advertsing**" (propaganda)). <u>**Nesse tipo de golpe são criados anúncios maliciosos e, por meio de serviços de publicidade, eles são apresentados em diversas páginas Web**</u>. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas.

Programas de distribuição de arquivos (P2P)

Permitem que os usuários compartilhem arquivos entre si. Exemplos: Kazaa, Gnutella e BitTorrent. O uso desses programas pode ocasionar: acessos indevidos a diretórios e arquivos se mal configurado, obtenção de arquivos maliciosos por meio dos arquivos distribuídos nesses ambientes, violação de direitos autorais (com distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais).

Compartilhamento de recursos

Ao fazer um compartilhamento de recursos do seu computador, como diretórios, discos, e impressoras, com outros usuários, pode estar permitindo:

- o acesso não autorizado a recursos ou informações sensíveis;
- que seus recursos sejam usados por atacantes caso não sejam definidas senhas para controle de acesso ou sejam usadas senhas facilmente descobertas.

Risco

RISCO é a medida da exposição à qual o sistema computacional está sujeito. Depende da probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque.

> Sêmola (2003, p. 50) diz que **risco é a "probabilidade de ameaças explorarem vulnerabilidades, provocando *perdas de confidencialidade, integridade e* disponibilidade, causando, possivelmente, impactos nos negócios**".

Como exemplo de um risco pode-se imaginar um funcionário insatisfeito e um martelo ao seu alcance; nesse caso o funcionário poderia danificar algum ativo da informação.

Existem algumas maneiras de se classificar o grau de risco no mercado de segurança, mas de uma forma simples, poderíamos tratar como alto, médio e baixo risco. No caso do nosso exemplo da sala dos servidores, poderíamos dizer que, baseado na vulnerabilidade encontrada, a ameaça associada é de alto risco.

Ciclo da Segurança

Como mostrado na figura seguinte os **ATIVOS** de uma organização precisam ser **protegidos**, pois estão sujeitos a **VULNERABILIDADES**.

Se as vulnerabilidades aumentam, aumentam-se os riscos permitindo a exploração por uma ameaça e a concretização de um ataque. Se estas ameaças crescem, aumentam-se ainda mais os riscos de perda da integridade, disponibilidade e confidencialidade da informação podendo causar impacto nos negócios.

Nesse contexto, **MEDIDAS DE SEGURANÇA** devem ser tomadas, os riscos devem ser analisados e diminuídos para que se estabeleça a segurança dos ativos da informação.

Figura. Ciclo da Segurança da Informação (MOREIRA, 2001)

Procedimentos de Segurança

Diante desse grande risco, uma série de procedimentos de segurança, considerados como "**boas práticas de segurança**" podem ser implementadas para salvaguardar os **ativos** da organização (CertBR, 2006).

Como podemos reduzir o volume de spam que chega até nossas caixas postais?

A resposta é bem simples! Basta ***navegar de forma consciente na rede***. Este conselho é o mesmo que recebemos para zelar pela nossa segurança no trânsito ou ao entrar e sair de nossas casas.

A seguir destacamos as principais dicas que foram reportadas pelo CertBr (2012) para que os usuários da Internet desfrutem dos recursos e benefícios da rede, com segurança:

- Preservar as informações pessoais, tais como: endereços de e-mail, dados pessoais e, principalmente, cadastrais de bancos, cartões de crédito e senhas. **Um bom exercício é pensar que ninguém forneceria seus dados pessoais a um estranho na rua, ok? Então, por que liberá-la na Internet?**

- Ter, sempre que possível, e-mails separados para assuntos pessoais, profissionais, para as compras e cadastros on-line. Certos usuários mantêm um e-mail somente para assinatura de listas de discussão.

No caso das promoções da Internet, geralmente, será necessário preencher formulários. **Ter um e-mail para cadastros on-line é uma boa prática para os usuários com o perfil descrito.** Ao preencher o cadastro, procure desabilitar as opções de recebimento de material de divulgação do site e de seus parceiros, pois justamente nesse item é que muitos usuários atraem spam, inadvertidamente!

- Não ser um "clicador compulsivo", ou seja, o usuário deve procurar controlar a curiosidade de verificar sempre a indicação de um site em um e-mail suspeito de spam. Pensar, analisar as características do e-mail e verificar se não é mesmo um golpe ou código malicioso.
- Não ser um "caça-brindes", "papa-liquidações" ou "destruidor-de-promoções", rs! Ao receber e-mails sobre brindes, promoções ou descontos, reserve um tempo para analisar o e-mail, sua procedência e verificar no site da empresa as informações sobre a promoção em questão. Vale lembrar que os sites das empresas e instituições financeiras têm mantido alertas em destaque sobre os golpes envolvendo seus serviços. Assim, a visita ao *site* da empresa pode confirmar a promoção ou alertá-lo sobre o golpe que acabou de receber por e-mail!
- **Ferramentas de combate ao *spam*** (**anti-spams**) são geralmente disponibilizadas do lado dos servidores de e-mail, filtrando as mensagens que são direcionadas à nossa caixa postal. Importante que se tenha um filtro anti-spam instalado, ou ainda, usar os recursos anti-spam oferecidos por seu provedor de acesso.
- Além do anti-spam, existem outras ferramentas bastante importantes para o usuário da rede: *anti-spyware*, firewall pessoal e antivírus, estudadas nesta aula.

Cuidados com Contas e Senhas

- **Uma senha pode ser descoberta** ao ser usada em computadores infectados; ao ser usada em *sites* falsos; por meio de tentativas de adivinhação; ao ser capturada enquanto trafega na rede, sem estar criptografada; por meio do acesso ao arquivo onde a senha foi armazenada caso ela não tenha sido gravada de forma criptografada; com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente; pela observação da movimentação dos seus dedos no teclado ou dos cliques do *mouse* em teclados virtuais (CERT.BR,2012).
- **Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você**

crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

- **Alguns** elementos que você **não deve** usar na elaboração de suas senhas são: **qualquer tipo de dado pessoal** (jamais utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você, etc.)**; sequências de teclado; palavras que façam parte de listas**.
- Alguns elementos que você **deve** usar na elaboração de suas senhas são: **números aleatórios; grande quantidade de caracteres; diferentes tipos de caracteres** (CERT.BR,2013).

  Mais dicas:
- crie uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos.
- utilize uma senha diferente para cada serviço (por exemplo, uma senha para o banco, outra para acesso à rede corporativa da sua empresa, outra para acesso a seu provedor de Internet etc.);
- altere a senha com frequência;
- crie tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- utilize o usuário *Administrator* (ou *root*) somente quando for estritamente necessário.

Cuidados com Malware

O combate a códigos maliciosos poderá envolver uma série de ações, como:

- instalação de ferramentas antivírus e antispyware no computador, lembrando de mantê-las atualizadas frequentemente. A banca pode citar ferramentas antimalware nesse contexto também;
- não realizar abertura de arquivos suspeitos recebidos por e-mail;
- fazer a instalação de patches de segurança e atualizações corretivas de softwares e do sistema operacional quando forem disponibilizadas
- (proteção contra worms e bots), etc.

***Vírus**

- Instale e mantenha atualizado um bom programa antivírus;
- atualize as assinaturas do antivírus, de preferência diariamente;

- configure o antivírus para verificar os arquivos obtidos pela Internet, discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*;
- desabilite no seu programa leitor de *e-mails* a auto-execução de arquivos anexados às mensagens;
- não execute ou abra arquivos recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus;
- utilize na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou *PostScript* etc.

*** Worms, bots e botnets**

- Siga todas as recomendações para prevenção contra vírus listadas no item anterior;
- mantenha o sistema operacional e demais *softwares* sempre atualizados;
- aplique todas as correções de segurança (*patches*) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos *softwares* utilizados;
- instale um *firewall* pessoal, que **em alguns casos** pode evitar que uma vulnerabilidade existente seja explorada **(observe que o firewall não corrige as vulnerabilidades!!)** ou que um *worm* ou *bot* se propague.

***Cavalos de troia, backdoors, keyloggers e spywares**

- Siga todas as recomendações para prevenção contra vírus, *worms* e *bots*;
- instale um *firewall* pessoal, que **em alguns casos** pode evitar o acesso a um *backdoor* já instalado em seu computador etc.;
- utilize pelo menos uma ferramenta anti-*spyware* e mantê-la sempre atualizada.

Cuidados com o seu dispositivo móvel

Ao usar seu dispositivo móvel (CERT.BR,2012)**:**

- se disponível, instale um programa *antimalware* antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;
- mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;
- fique atento às notícias veiculadas no *site* do fabricante, principalmente as relacionadas à segurança;

- seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e *plug-ins*;
- seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isto pode comprometer a sua privacidade

Ao acessar redes (CERT.BR,2013)**:**

- seja cuidadoso ao usar redes Wi-Fi públicas;
- mantenha interfaces de comunicação, como *bluetooth*, infravermelho e Wi-Fi, desabilitadas e somente as habilite quando for necessário;
- configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").
- **Proteja seu dispositivo móvel e os dados nele armazenados** (CERT.BR,2013):
    - mantenha as informações sensíveis sempre em formato **criptografado**;
    - faça ***backups* periódicos** dos dados nele gravados;
    - mantenha **controle físico** sobre ele, principalmente em locais de risco (procure não deixá-lo sobre a mesa e cuidado com bolsos e bolsas quando estiver em ambientes públicos);
    - use **conexão segura** sempre que a comunicação envolver dados confidenciais;
    - não siga *links* recebidos por meio de mensagens eletrônicas;
    - cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas);
    - configure-o para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto);
    - configure-o, quando possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso (use esta opção com bastante cautela, principalmente se você tiver filhos e eles gostarem de "brincar" com o seu dispositivo).

Elaboração de uma Política de Segurança com o objetivo de solucionar ou minimizar as vulnerabilidades encontradas na organização.

Nesse contexto, dos principais itens necessários para uma boa política de segurança pode-se citar os seguintes:

- Possuir instalações físicas adequadas que ofereçam o mínimo necessário para garantia da integridade dos dados.

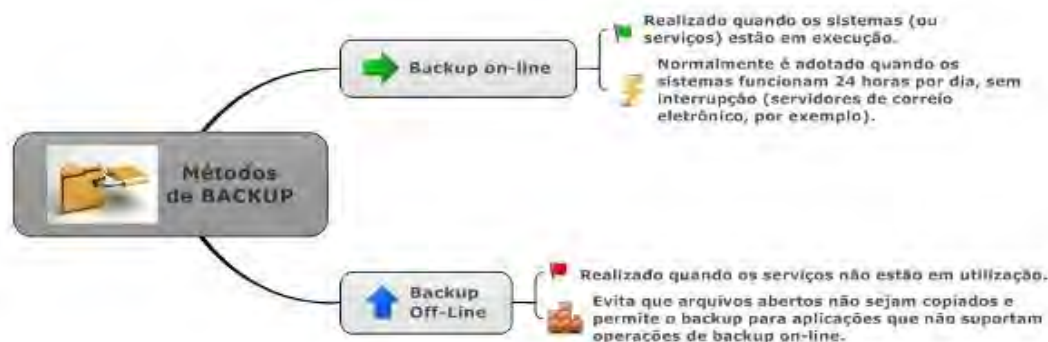
- Controle de umidade, temperatura e pressão.
- Sistema de aterramento projetado para suportar as descargas elétricas, extintores de incêndio adequados para equipamentos elétricos/eletrônicos.
- Uso adequado de equipamentos de proteção e segurança tais como: UPS (*"no-break"*), filtro de linha, estabilizador de tensão.
- Manutenção do computador, limpeza e política da boa utilização.
- Utilização de sistemas operacionais que controlem o acesso de usuários e que possuem um nível de segurança bem elaborado, juntamente com o controle de senhas.
- Utilização de sistemas de proteção de uma rede de computadores, tais como **Firewall** (sistema que filtra e monitora as ações na rede).
- Software antivírus atualizado constantemente.
- Sistema de **criptografia** (ferramenta que garante a segurança em todo ambiente computacional que precise de sigilo em relação às informações que manipula). No envio de mensagens uma mensagem é criptografada e se for interceptada dificilmente poderá ser lida, somente o destinatário possuir o código necessário.
- **Treinamento** e conscientização de funcionários para diminuir as falhas humanas.
- Realização de ***backups*** (cópia de segurança **para salvaguardar os dados, geralmente mantida em CDs, DVDs, fitas magnéticas, pendrives, etc., para que possam ser restaurados em caso de perda dos dados originais**).

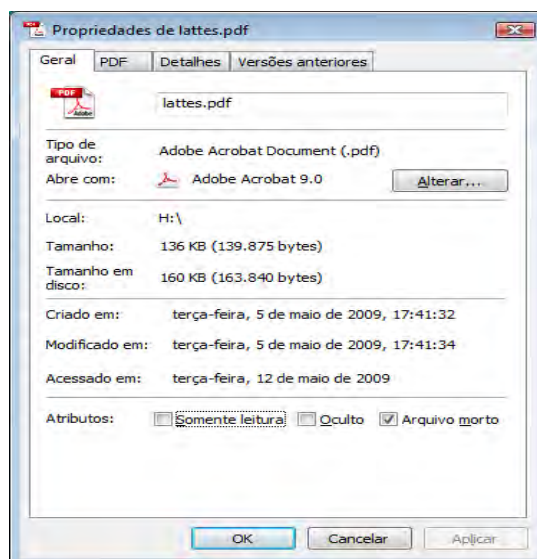
Procedimentos de Backup (Cópia de segurança)

O procedimento de **backup (cópia de segurança)** pode ser descrito de forma simplificada como **copiar dados de um dispositivo para o outro com o objetivo de posteriormente recuperar as informações, caso haja algum problema**.

Um **backup** envolve cópia de dados em um meio fisicamente separado do original, regularmente, de forma a protegê-los de qualquer eventualidade. Assim, copiar nossas fotos digitais, armazenadas no HD (disco rígido), para um DVD é fazer backup. Se houver algum problema com o HD ou se acidentalmente apagarmos as fotos, podemos então restaurar os arquivos a partir do DVD. Nesse exemplo, chamamos as cópias das fotos no DVD de cópias de segurança ou backup. Chamamos de **restauração o processo de copiar de volta ao local original as cópias de segurança**.

É importante estabelecer uma **política de backup** que obedece a critérios bem definidos sobre a segurança da informação envolvida. Em suma, o objetivo principal dos backups é garantir a **disponibilidade** da informação. Por isso a política de backup é um processo relevante no contexto de segurança dos dados.

Existem, basicamente, **dois métodos de Backup**.

No Windows XP, por exemplo, tem-se o software Microsoft Backup, que irá ajudá-lo nesta tarefa. Ao clicar com o botão direito do mouse no ícone de um arquivo do Windows XP, e selecionar a opção Propriedades; em seguida, guia geral ->Avançado, será exibida uma caixa "*o arquivo está pronto para ser arquivado*", marcada como padrão (No Windows XP, leia-se arquivo morto).

A tela seguinte desta a opção de "arquivo morto" obtida ao clicar com o botão direito do mouse no arquivo intitulado lattes.pdf, do meu computador que possui o sistema operacional Windows Vista.

→ Quando um **arquivo está com esse atributo marcado, significa que ele deverá ser copiado no próximo backup**.

→ Se estiver desmarcado, significa que, provavelmente, já foi feito um backup deste arquivo.

As principais **técnicas (tipos) de Backup**, que podem ser combinadas com os mecanismos de backup on-line e off-line, estão listadas a seguir:

****NORMAL (TOTAL ou GLOBAL)**

- **COPIA TODOS** os arquivos e pastas selecionados.
- **DESMARCA o atributo de arquivo morto** (arquivamento): limpa os marcadores!!
- Caso necessite restaurar o backup normal, você só precisa da cópia mais recente.
- Normalmente, este *backup* é executado quando você cria um conjunto de *backup* pela 1ª vez.
- Agiliza o processo de restauração, pois somente um backup será restaurado.

****INCREMENTAL**

- **Copia somente os arquivos CRIADOS ou ALTERADOS desde o último backup <u>normal</u> ou <u>incremental</u>.**
- O atributo de arquivamento (arquivo morto) **É DESMARCADO**: limpa os marcadores!!

Resumindo: A estratégia de backup Incremental é:
- Mais rápida para fazer o backup, pois copia poucos arquivos por dia;
- Mais demorada para fazer a restauração, pois é necessário restaurar diversas fitas.

****DIFERENCIAL**

- Copia somente os arquivos **CRIADOS** ou **ALTERADOS desde o último backup normal ou incremental**.
- O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO**: não limpa os marcadores!!

Observe que o backup diferencial é acumulativo, ou seja, em cada fita de backup sempre estarão inclusos os arquivos que foram modificados desde o último backup full (normal).

Resumindo: A estratégia de backup Diferencial é:
- Mais demorada para fazer o backup, pois copia cada arquivo que foi alterado a contar do último backup full (normal) realizado;
- Mais rápida para fazer a restauração, pois é necessário restaurar somente dois dias de backup (O full e o dia anterior ao crash).

****CÓPIA (AUXILIAR ou SECUNDÁRIA)**

- Faz o backup de arquivos e pastas selecionados.
- O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO**: não limpa os marcadores!

****DIÁRIO**

- Copia todos os arquivos e pastas selecionados que foram **ALTERADOS DURANTE O DIA** da execução do backup.
- O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO:** não limpa os marcadores!

Tipo de Backup	Dados Copiados	Ação após a cópia
Total ou Global Normal	Copia todos os arquivos selecionados	Marca todos os arquivos como copiados.
Incremental	Copia os arquivos novos ou alterados desde o último Backup total ou Incremental.	Marca todos os arquivos como copiados.
Diferencial	Copia os arquivos novos ou alterados desde o último Backup Global ou Incremental.	Não marca nada.
Diário	Copia os arquivos criados ou alterados no dia.	Não marca nada.
Cópia	Copia todos os arquivos selecionados.	Não marca nada.

Quanto à RECUPERAÇÃO do backup:

→ Para recuperar um disco a partir de um conjunto de *backups* (normal + **incremental**) será necessário o primeiro (normal) e todos os incrementais.

→ Para recuperar um disco a partir de um conjunto de *backups* (normal + **diferencial**) basta o primeiro (normal) e o último diferencial, já que este contém tudo que é diferente do primeiro.

Aplicativos para Aprimoramento da Segurança

**Antivírus

Ferramentas preventivas e corretivas, que detectam (e, em muitos casos, removem) vírus de computador e outros programas maliciosos (como spywares e cavalos de troia).

Não impedem que um atacante explore alguma vulnerabilidade existente no computador. Também não evita o acesso não autorizado a um *backdoor* instalado no computador.

Dicas!!

É interessante manter, em seu computador:

- Um antivírus funcionando constantemente (preventivamente).
- Esse programa antivírus verificando os e-mails constantemente (preventivo).
- O recurso de atualizações automáticas das definições de vírus habilitado.
- As definições de vírus atualizadas constantemente (nem que para isso seja necessário, todos os dias, executar a atualização manualmente).

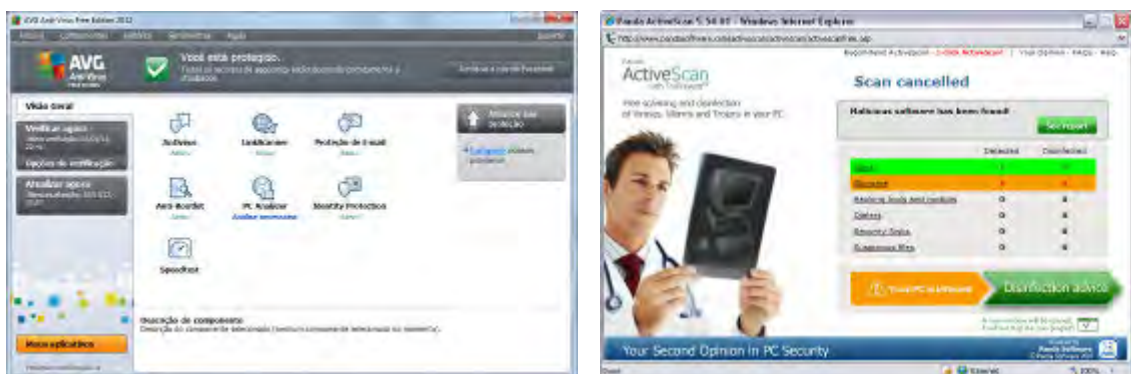



Figura. Telas do antivírus AVG e Panda

Figura. Panda Cloud Antivírus => Usa a "nuvem de Internet" como recurso para proteger o computador do usuário.

**AntiSpyware

O malware do tipo spyware pode se instalar no computador sem o seu conhecimento e a qualquer momento que você se conectar à Internet, e pode infectar o computador quando você instala alguns programas usando um CD, DVD ou outra mídia removível. Um spyware também pode ser programado para ser executado em horários inesperados, não apenas quando é instalado.

A ferramenta antispyware é uma forte aliada do antivírus, permitindo a localização e bloqueio de spywares conhecidos e desconhecidos. Exemplo de ferramentas antispyware: Windows Defender, Spybot etc.

**IPS/IDS, Firewalls

O **IDS (*Intrusion Detection Systems*)** procura por ataques já catalogados e registrados, podendo, em alguns casos, fazer análise comportamental do sistema.

O **IPS** (**Sistema de Prevenção de Intrusão**) é que faz a detecção de ataques e intrusões, e não o *firewall*!! Um IPS é um sistema que detecta e obstrui automaticamente ataques computacionais a recursos protegidos. Diferente dos IDS tradicionais, que localizam e notificam os administradores sobre anomalias, um IPS defende o alvo sem uma participação direta humana.

> **O firewall não tem a função de procurar por ataques. Ele realiza a filtragem dos pacotes e, então, bloqueia as transmissões não permitidas.** Dessa forma, atua entre a rede externa e interna, controlando o tráfego de informações que existem entre elas, procurando certificar-se de que este tráfego é confiável, em conformidade com a política de segurança do site acessado. Também pode ser utilizado para atuar entre redes com necessidades de segurança distintas.

A RFC 2828 (*Request for Coments* nº 2828) define o termo ***firewall*** como sendo uma **ligação entre redes de computadores que restringe o tráfego de comunicação de dados entre a parte da rede que está "dentro" ou "antes" do firewall, protegendo-a assim das ameaças da rede de computadores que está "fora" ou depois do firewall**. Esse mecanismo de proteção geralmente é utilizado para proteger uma rede menor (como os computadores de uma empresa) de uma rede maior (como a Internet).

Um *firewall* deve ser instalado no ponto de conexão entre as redes, onde, através de regras de segurança, controla o tráfego que flui para dentro e para fora da rede protegida. **Pode ser desde um único computador, um software sendo executado no ponto de conexão entre as redes de computadores ou um conjunto complexo de equipamentos e softwares**.

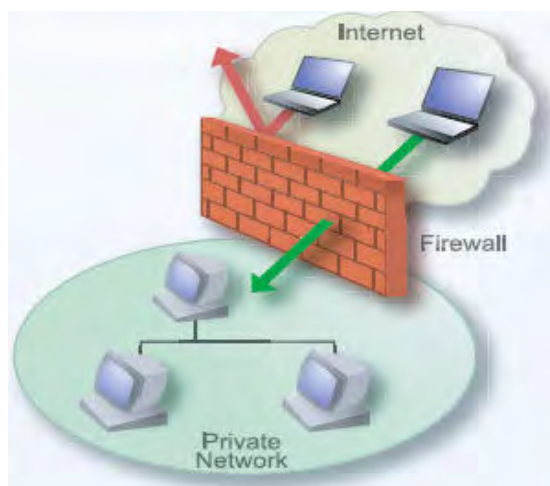



Figura. Firewall

Deve-se observar que isso o torna um potencial gargalo para o tráfego de dados e, caso não seja dimensionado corretamente, poderá causar atrasos e diminuir a *performance* da rede.

Os firewalls são implementados, em regra, em dispositivos que fazem a separação da rede interna e externa, chamados de **estações guardiãs** (***bastion hosts***). Quando o *bastion host* cai, a conexão entre a rede interna e externa pára de funcionar.

As principais funcionalidades oferecidas pelos *firewalls* são:

- regular o tráfego de dados entre uma rede local e a rede externa não confiável, por meio da introdução de filtros para pacotes ou aplicações;
- impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados dentro de uma rede local;
- mecanismo de defesa que restringe o fluxo de dados entre redes, podendo criar um "log" do tráfego de entrada e saída da rede;
- proteção de sistemas vulneráveis ou críticos, ocultando informações de rede como nome de sistemas, topologia da rede, identificações dos usuários etc.

DMZ - Zona Desmilitarizada

Também chamada de **Rede de Perímetro**. Trata-se de **uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.**

A função de uma DMZ é **manter todos os serviços que possuem acesso externo (navegador, servidor de e-mails) separados da rede local** limitando o dano em caso de comprometimento de algum serviço nela presente por algum invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma rota de acesso à rede local. O termo possui uma origem militar, significando a área existente entre dois inimigos em uma guerra.

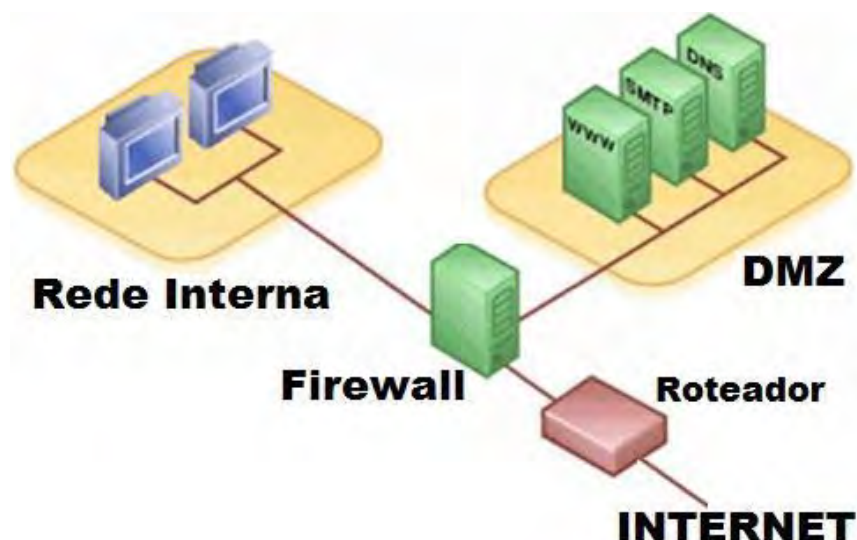



Figura. DMZ

RAID - *Redundant Array of Independent Disks*
(Matriz redundante de discos independentes)

Tecnologia utilizada para combinar diversos discos rígidos (IDE, SATA ou SCSI) para que sejam reconhecidos, pelo sistema operacional, como apenas UMA única unidade de disco. Existem vários tipos (chamados "**modos"**) de RAID, e os mais comuns são:

RAID 0 (*Stripping* - Enfileiramento)

- Cada modo desses combina os discos rígidos de formas diferentes para obterem resultados diferentes.
- Combina dois (ou mais) HDs para que os dados gravados sejam divididos entre eles.
- No caso de um RAID 0 entre dois discos, os arquivos salvos nesse conjunto serão gravados METADE em um disco, METADE no outro.
- Ganha-se muito em **velocidade**
  - a **gravação** do arquivo é feita em metade do tempo, porque se grava metade dos dados em um disco e metade no outro simultaneamente (o barramento RAID é outro, separado, do IDE).
  - A **leitura** dos dados dos discos também é acelerada!
  - Nesse RAID **não há tolerância a falhas (segurança)** porque de um dos discos "pifar", os dados estarão perdidos completamente.
  - Não se preocupa com segurança e sim com a velocidade!

RAID 1 (Mirroring - Espelhamento)

- Cria uma matriz (array) de discos espelhados (discos idênticos). O que se copia em um, copia-se igualmente no outro disco.
- O RAID 1 aumenta a segurança do sistema.
- RAID 1 aumenta a velocidade de leitura dos dados no disco (não a de escrita).

RAID 5

- Sistema **tolerante a falhas**, cujos dados e paridades são distribuídos ao longo de três ou mais discos físicos.
- A paridade é um valor calculado que é usado para reconstruir dados depois de uma falha.
- Se um disco falhar, é possível recriar os dados que estavam na parte com problema a partir da paridade e dados restantes.

Biometria

Um sistema biométrico, em mecanismos de **autenticação**, analisa uma amostra de corpo do usuário, envolvendo por exemplo: Impressão Digital (+usado); Íris; Voz; Veias das Mãos; Reconhecimento Facial (+usado).

Figura 2 Veias da palma da mão, impressão digital, reconhecimento da face, identificação pela íris ou retina, geometria da mão, etc.

Virtual Private Network (VPN)

Uma **Virtual Private Network (VPN) ou Rede Virtual Privada** é uma rede privada (rede com acesso restrito) construída sobre a estrutura de uma rede pública (recurso público, sem controle sobre o acesso aos dados), normalmente a Internet. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes para conectar redes remotas, utiliza-se a infraestrutura da Internet, uma vez que para os usuários a forma como as redes estão conectadas é transparente.

Normalmente as VPNs são utilizadas para interligar empresas em que os custos de linhas de comunicação direta de dados são elevados. Elas criam "túneis" virtuais de transmissão de dados utilizando criptografia para garantir a privacidade e integridade dos dados, e a autenticação para garantir que os dados estão sendo transmitidos por entidades ou dispositivos autorizados e

não por outros quaisquer. Uma VPN pode ser criada tanto por dispositivos específicos, softwares ou até pelo próprio sistema operacional.

Princípios básicos (Caiu em prova!)

Uma VPN deve prover um conjunto de funções que garantam alguns princípios básicos para o tráfego das informações:

1. Confidencialidade – tendo-se em vista que estarão sendo usados meios públicos de comunicação, é imprescindível que a privacidade da informação seja garantida, de forma que, mesmo que os dados sejam capturados, não possam ser entendidos.

2. Integridade – na eventualidade da informação ser capturada, é necessário garantir que não seja alterada e reencaminhada, permitindo que somente informações válidas sejam recebidas.

3. Autenticidade – somente os participantes devidamente autorizados podem trocar informações entre si, ou seja, um elemento da VPN somente reconhecerá informações originadas por um segundo elemento que tenha autorização para fazer parte dela.

Criptografia

A palavra **criptografia** é composta dos termos gregos KRIPTOS (secreto, oculto, ininteligível) e GRAPHO (escrita, escrever). Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la.

Terminologia básica sobre Criptografia:

- **Mensagem ou texto:** Informação que se deseja proteger. Esse texto quando em sua forma original, ou seja, a ser transmitido, é chamado de **texto puro** ou **texto claro**.
- **Remetente ou emissor:** Pessoa que envia a mensagem.
- **Destinatário ou receptor:** Pessoa que receberá a mensagem.
- **Encriptação:** Processo em que um texto puro passa, transformando-se em **texto cifrado**.
- **Desencriptação:** Processo de recuperação de um **texto puro** a partir de um **texto cifrado**.
- **Criptografar:** Ato de **encriptar** um **texto puro**, assim como, **descriptografar** é o ato de **desencriptar** um **texto cifrado**.
- **Chave:** Informação que o remetente e o destinatário possuem e que será usada para criptografar e descriptografar um texto ou mensagem.

Algoritmos:

→ **Simétricos** (ou convencional, chave privada, chave única)

→ **Assimétricos** (ou chave pública).

Criptografia de <u>Chave Simétrica</u> (também chamada de criptografia de chave única, ou criptografia privada, ou criptografia convencional)

Utiliza **APENAS UMA** chave para encriptar e decriptar as mensagens. Assim, como só utiliza UMA chave, obviamente ela deve ser compartilhada entre o remetente e o destinatário da mensagem.

Para ilustrar os sistemas simétricos, podemos usar a imagem de um cofre, que só pode ser fechado e aberto com uso de uma chave. Esta pode ser, por exemplo, uma combinação de números. A mesma combinação abre e fecha o cofre.

<u>*Para criptografar uma mensagem, usamos a chave (fechamos o cofre) e para decifrá-la utilizamos a mesma chave (abrimos o cofre).*</u>

Na criptografia simétrica (ou de chave única) tanto o emissor quanto o receptor da mensagem devem conhecer a chave utilizada!! Ambos fazem uso da MESMA chave, isto é, uma ÚNICA chave é usada na codificação e na decodificação da informação.

A figura seguinte ilustra o processo de criptografia baseada em uma única chave, ou seja, a chave que cifra uma mensagem é utilizada para posteriormente decifrá-la.

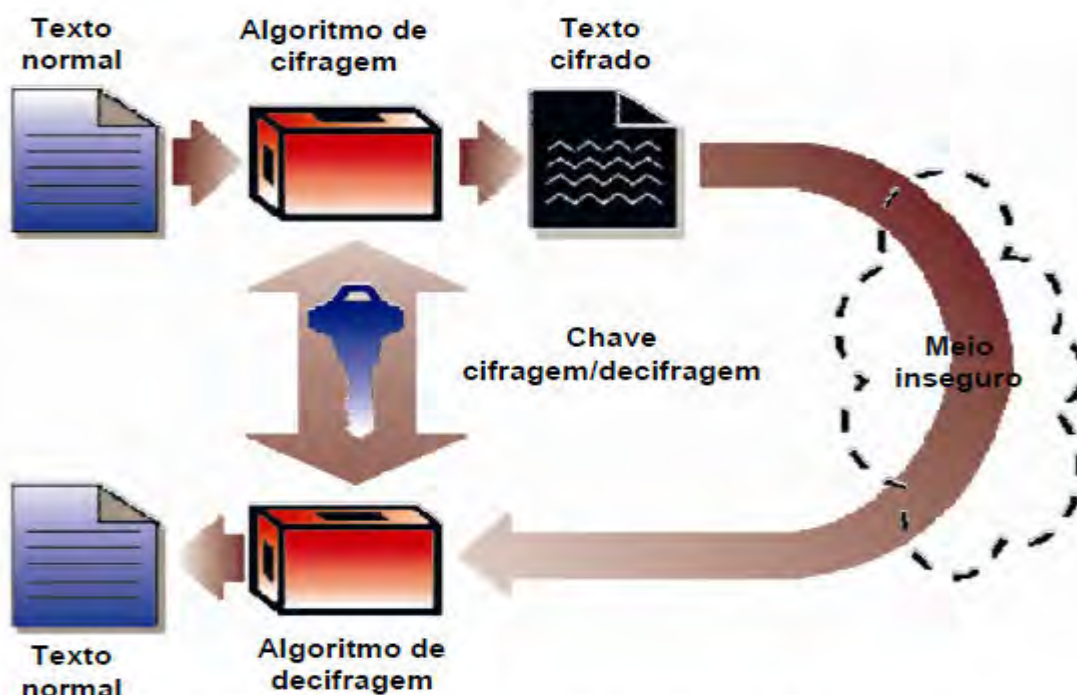



Ilustração de um processo de criptografia por chave secreta.
Fonte: GARFINKEL, Simson; SPAFFORD, Gene (1999, p. 197)

As principais **vantagens** dos **algoritmos simétricos** são:

- rapidez: um polinômio simétrico encripta um texto longo em milésimos de segundos;
- chaves pequenas: uma chave de criptografia de 128 bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior **desvantagem** da criptografia simétrica é que a chave utilizada para encriptar é IGUAL à chave que decripta. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

O uso de chaves simétricas também faz com que sua utilização não seja adequada em situações em que a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas estejam envolvidas. Ainda, há o fato de que tanto o emissor quanto o receptor precisam conhecer a chave usada.

A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas", fazendo com que a chave possa ser interceptada e/ou alterada em trânsito por um inimigo.

Existem vários algoritmos que usam chaves simétricas, como o **DES** (Data Encryption Standard), o **IDEA** (International Data Encryption Algorithm), e o **RC** (Ron's Code ou Rivest Cipher).

Criptografia de Chave ASSimétrica (também chamada de criptografia de chave pública)

Os algoritmos de **criptografia assimétrica (criptografia de chave pública)** utilizam **DUAS** chaves **DIFERENTES**, uma **PÚBLICA** (que pode ser distribuída) e uma **PRIVADA** (pessoal e intransferível). Assim, nesse método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono.

As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Do ponto de vista do custo computacional, **os sistemas simétricos apresentam melhor desempenho que os sistemas assimétricos**, e isso já foi cobrado em provas várias vezes!

A figura seguinte ilustra o princípio da criptografia utilizando chave assimétrica.

Também conhecida como "**chave pública**", a técnica de **criptografia por chave assimétrica** trabalha com **DUAS chaves**: **uma denominada privada e outra denominada pública**. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Outra chave deve ser criada para a decodificação. Esta – a chave privada – é secreta.

Ilustração de um processo de criptografia por chave pública
Fonte: GARFINKEL, Simson; SPAFFORD, Gene (2001, p.208).

Para entender melhor, imagine o seguinte: o USUÁRIO-A criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao USUÁRIO-A deverá utilizar a chave pública deste. Quando o USUÁRIO-A receber a informação, apenas será possível extraí-la com o uso da chave privada, que só o USUÁRIO-A tem. Caso o USUÁRIO-A queira enviar uma informação criptografada a outro site, deverá conhecer sua chave pública.

Entre os algoritmos que usam chaves assimétricas têm-se o **RSA** (o mais conhecido), o Diffie-Hellman, o **DSA** (Digital Signature Algorithm), o Schnorr (praticamente usado apenas em assinaturas digitais) e **Diffie-Hellman**.

Figura. Mapa mental relacionado à Criptografia ASSimétrica

PKI (Public Key Infrastrusture) é a infraestrutura de chaves públicas (ICP). A ICP-Brasil é um exemplo de PKI.

Assinatura Digital

O glossário criado pela ICP Brasil destaca que a **Assinatura Digital é um código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um *e-mail* ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.**

Stallings (2008) destaca que a **assinatura digital é um mecanismo de AUTENTICAÇÃO** que permite ao criador de uma mensagem anexar um código que atue como uma assinatura.

Em outras palavras, a assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

A assinatura é formada tomando o *hash* da mensagem e criptografando-a com a chave privada do criador. **A assinatura garante a ORIGEM e a INTEGRIDADE da mensagem.**

HASH (Message Digest – Resumo de Mensagem): Método matemático "**unidirecional**", ou seja, só pode ser executado em um único sentido (ex.: você envia uma mensagem com o hash, e este não poderá ser alterado, mas apenas conferido pelo destinatário). Utilizado para garantir a "integridade" (não alteração) de dados durante uma transferência.

Se José quiser enviar uma mensagem assinada para Maria, ele codificará a mensagem com sua chave privada. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria utilizará a chave pública de José para decodificar a mensagem. Neste processo será gerada uma segunda assinatura digital, que será comparada à primeira. Se as assinaturas forem idênticas, Maria terá certeza que o remetente da mensagem foi o José e que a mensagem não foi modificada.

É importante ressaltar que a segurança do método baseia-se no fato de que **a chave privada é conhecida apenas pelo seu dono**. Também é importante ressaltar que o fato de **assinar uma mensagem não significa gerar uma mensagem sigilosa**. Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

Certificado Digital

Um certificado digital é um **documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores (computadores)** dentre outras entidades. Este "documento" na verdade é uma **estrutura de dados** que contém a chave pública do seu titular e outras informações de interesse. Contêm informações relevantes para a identificação "real" da entidade a que visam certificar (CPF, CNPJ, endereço, nome, etc.) e informações relevantes para a aplicação a que se destinam. O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação. Chamamos essa autoridade de **Autoridade Certificadora,** ou **AC**.

O certificado fica armazenado em **dispositivos de segurança**, como por ex.: *Token* ou *Smart Card*, ilustrados na figura a seguir.

Token

Smart Card ou cartão inteligente

Figura. Ilustração de dispositivos de segurança

Quanto aos objetivos do certificado digital podemos destacar:

- Transferir a credibilidade que hoje é baseada em papel e conhecimento para o ambiente eletrônico.
- **Vincular uma chave pública a um titular** (eis o objetivo principal). O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação, conforme visto na próxima figura. Chamamos essa autoridade de **Autoridade Certificadora**, ou **AC**.

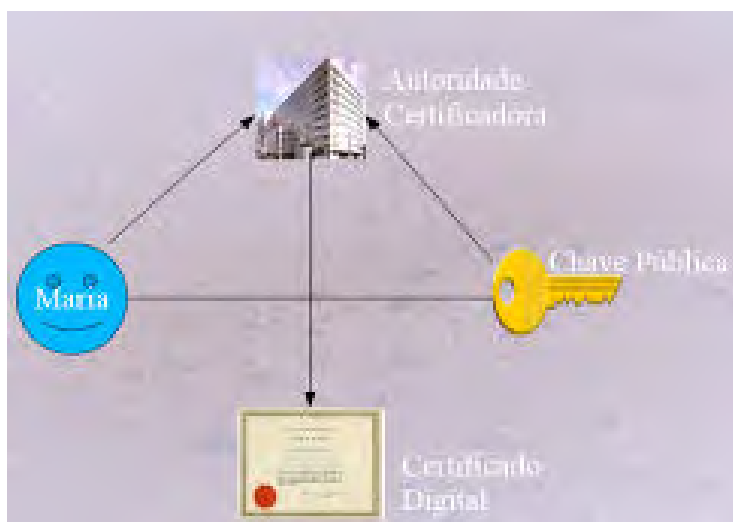
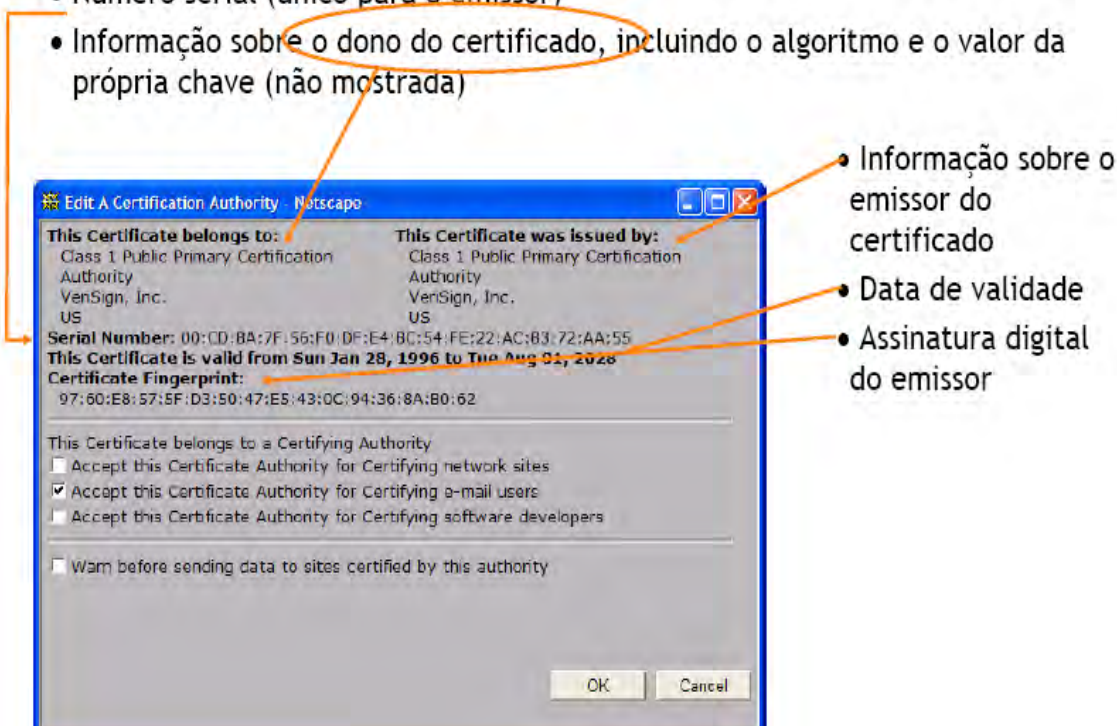



Figura. Vínculo da Chave Pública ao Titular

Dentre as **informações que compõem a estrutura de um certificado** temos:

Versão	Indica qual formato de certificado está sendo seguido.
Número de série	Identifica unicamente um certificado dentro do escopo do seu emissor.
Nome do titular	Nome da pessoa, URL ou demais informações que estão sendo certificadas.
Chave pública do titular	Informações da chave pública do titular.
Período de validade	Data de emissão e expiração.
Nome do emissor	Entidade que emitiu o certificado.
Assinatura do emissor	Valor da assinatura digital feita pelo emissor.
Algoritmo de assinatura do emissor	Identificador dos algoritmos de *hash* + assinatura utilizados pelo emissor para assinar o certificado.
Extensões	Campo opcional para estender o certificado.

Um exemplo destacando informações do certificado pode ser visto na figura seguinte:

Certificação Digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

Esse reconhecimento é inserido em um **Certificado Digital**, por uma **Autoridade Certificadora**.

MEMOREX -> Direto ao PONTO!

- **Engenharia Social:** Técnica de ataque que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia.
- ***Malwares*** (combinação de *malicious software* – *programa malicioso*)**: programas que executam deliberadamente ações mal-intencionadas em um computador, como vírus, *worms*, *bots*, cavalos de troia, *spyware*, *keylogger*, *screenlogger*.**

- **Não repúdio**: Garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação. Transações digitais estão sujeitas a fraude, quando sistemas de Com putador são acessados indevidamente ou infectados por cavalos de troia ou vírus. Assim os participantes podem, potencialmente, alegar fraude para repudiar uma transação.
- **Phishing** ou **scam:** Tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente.
- **Pharming**: Ataque que consiste em corromper o DNS em uma rede de computadores, fazendo com que a URL de um site passe a apontar para o IP de um servidor diferente do original.
- No **ataque de negação de serviço (*denial of service* - DoS)** o atacante utiliza um computador para tirar de operação um serviço ou computador(es) conectado(s) à Internet!!

- No **ataque de negação de serviço distribuído (DDoS)** um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.
- **Spams:** Mensagens de correio eletrônico não autorizadas ou não solicitadas pelo destinatário, geralmente de conotação publicitária ou obscena.
- **Sniffer**: Ferramenta capaz de interceptar e registrar o tráfego de dados em uma rede de computadores.
- **Botnets**: Redes formadas por diversos computadores infectados com bots ("**Redes Zumbis**"). Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de spam, etc.
- ***Firewall***: Um sistema para controlar o acesso às redes de computadores, desenvolvido para evitar acessos não autorizados em uma rede local ou rede privada de uma corporação.
- **VPN** (***Virtual Private Network* – Rede Privada Virtual**): **Rede privada** que usa a estrutura de uma rede **pública** (como a **Internet**) para transferir seus dados (os dados devem estar **criptografados** para passarem despercebidos e inacessíveis pela Internet).
- **Vulnerabilidade:** Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque. Ex.: notebook sem as atualizações de segurança do sistema operacional.
- Princípios básicos da segurança da informação:

Princípio básico	Conceito	Objetivo
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.	Proteger contra o acesso não autorizado, mesmo para dados em trânsito.
Integridade	Propriedade de salvaguarda da exatidão e completeza de ativos.	Proteger informação contra modificação sem permissão; garantir a fidedignidade das informações.
Disponibilidade	Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.	Proteger contra indisponibilidade dos serviços (ou degradação); garantir aos usuários com autorização, o acesso aos dados.

- **Anti-spam:** Ferramenta utilizada para filtro de mensagens indesejadas.

- Existem vários tipos de RAID (***Redundant Array of Independent Disks)***, e os mais comuns são: **RAID 0**, **RAID 1,** RAID 10 (também conhecido como 1+0) e **RAID 5.**
- ***Backup* (cópia de segurança):** envolve a cópia dos dados de um dispositivo para o outro com o objetivo de posteriormente recuperar as informações, caso haja algum problema. Procure fazer cópias regulares dos dados do computador, para recuperar-se de eventuais falhas e das consequências de uma possível infecção por vírus ou invasão.

  Principais **tipos** de **backup**:

INCREMENTAL	CÓPIA (AUXILIAR ou SECUNDÁRIA)	DIÁRIO
• **Copia somente os arquivos CRIADOS ou ALTERADOS desde o último backup normal ou incremental.** • O atributo de arquivamento (arquivo morto) **É DESMARCADO.**	• **COPIA TODOS** os arquivos selecionados, assim como no backup normal. • O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO.**	• Copia todos os arquivos selecionados que foram **ALTERADOS NO DIA** da execução do backup. • O atributo de arquivamento (arquivo morto) **NÃO É ALTERADO.**

Estratégias de backup

Backup Incremental	Backup Diferencial
-Mais rápido para realizar o backup -Mais demorado para restaurar os dados	-Mais demorado para realizar o backup -Mais rápido para restaurar os dados

RAID não é backup!

- **RAID** – Medida de redundância.
- **Backup** – Medida de recuperação de desastre.

- ***HASH (Message Digest – Resumo de Mensagem):*** Método matemático "**unidirecional**", ou seja, só pode ser executado em um único sentido (ex.: você envia uma mensagem com o hash, e este não poderá ser alterado, mas apenas conferido pelo destinatário). Utilizado para garantir a "integridade" (não-alteração) de dados durante uma transferência.

Muito bem, após termos visto os conceitos primordiais de segurança para a prova, vamos às questões!!

LISTA DE QUESTÕES COMENTADAS

1. **(CESPE/2013/TRT-10RJ/Analista)** A transferência de arquivos para pendrives constitui uma forma segura de se realizar becape, uma vez que esses equipamentos não são suscetíveis a malwares.

Comentários

Antes de responder a afirmação é importante saber que os softwares maliciosos, ou **malwares**, têm o objetivo de provocar danos ao sistema. Dentro desse grupo temos os vírus, que são programas que atuam sobre outros programas, como uma aplicação ou mesmo um registro do sistema, e modificam seu comportamento e consequentemente provocam danos dos mais diversos.

Com a popularização dos pendrives, desenvolvedores de softwares começaram a produzir versões portáteis das aplicações (programas), incluindo os programas maliciosos (malwares). Logo a afirmação está incorreta pois dispositivos como pendrives, apesar de práticos e úteis em backups (cópias de segurança) não são imunes aos malwares.

Gabarito preliminar: item errado.

2. **(CESPE/2013/TRT-10RJ/Analista)** As características básicas da segurança da informação — confidencialidade, integridade e disponibilidade — não são atributos exclusivos dos sistemas computacionais.

Comentários

Essas características (também conhecidas como atributos ou princípios) atuam sobre quaisquer ativos de segurança da informação, que é o que a segurança da informação quer proteger, como servidores, estações de trabalho, sistemas computacionais, etc.

Gabarito preliminar: item correto.

3. **(CESPE/2013/TRT-10RJ/Analista)** O vírus de computador é assim denominado em virtude de diversas analogias poderem ser feitas entre esse tipo de vírus e os vírus orgânicos.

Comentários

Primeiro vamos entender que um vírus de computador é um programa criado do mesmo modo que os outros programas, ou seja, trata-se de um conjunto de instruções que determinam o que o computador deve fazer, e esses programas contém ordens específicas como modificar outros programas, alterar arquivos e/ou causar várias outras anomalias.

O vírus orgânico é uma partícula infecciosa muito pequena constituída de DNA ou RNA (ácidos nucleicos presentes na composição dos seres vivos) que causam alteração em seu hospedeiro.

Percebeu a semelhança?

- Ambos se instalam em um organismo/sistema.
- Ambos causam alteração no organismo/sistema hospedeiro.
- Ambos são compostos por unidades semelhantes aos de seus hospedeiros (DNA ou RNA para o vírus orgânico e instruções para o vírus de computador).

Gabarito preliminar: item correto.

4. **(CESPE/2013/TRT-10RJ/Analista)** Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

Comentários

Afirmação correta, porque se você se conecta à Internet, ou permite que outras pessoas usem seu computador ou compartilha arquivos com outros computadores você está suscetível a ataques tanto diretos dos criminosos virtuais ou indiretamente porque esses criminosos criam softwares mal-intencionados com a finalidade de roubar dados ou mesmo danificar seu computador.

Os programas antivírus verificam a existência desses softwares maliciosos em emails e outros arquivos e como os malwares são atualizados constantemente o banco de dados do antivírus deve sempre estar atualizado porque quando o programa é atualizado as informações sobre novos vírus são adicionadas a uma lista de vírus a serem verificados, ajudando a proteger o seu computador contra novos ataques. Se a lista de vírus estiver desatualizada, o computador ficará vulnerável a novas ameaças.

Gabarito preliminar: item correto.

5. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Para garantir que os computadores de uma rede local não sofram ataques vindos da Internet, é necessária a instalação de firewalls em todos os computadores dessa rede.

Comentários

O **firewall** é um mecanismo que atua como "defesa" de um computador ou de uma rede, permitindo controlar o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de firewalls em redes é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

Gabarito: item errado.

6. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Ao se realizar um procedimento de backup de um conjunto de arquivos e pastas selecionados, é possível que o conjunto de arquivos e pastas gerado por esse procedimento ocupe menos espaço de memória que aquele ocupado pelo conjunto de arquivos e pastas de que se fez o backup.

Comentários

Alguns programas que realizam o backup de um determinado conjunto de arquivos e pastas podem oferecer a possibilidade de se realizar a compactação dos dados originais com a finalidade de se reduzir o espaço ocupado na mídia de destino.

Gabarito: item correto.

7. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Os worms, assim como os vírus, infectam computadores, mas, diferentemente dos vírus, eles não precisam de um programa hospedeiro para se propagar.

Comentários

Tantos os Worms como os vírus são considerados como malwares (softwares maliciosos que infectam computadores), no entanto, diferentemente do vírus, o Worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.

Gabarito: item correto.

8. **(CESPE/Técnico Administrativo – Nível Médio – PREVIC/2011)** Entre os atributos de segurança da informação, incluem-se a confidencialidade, a integridade, a disponibilidade e a autenticidade. A integridade consiste na propriedade que limita o acesso à informação somente às pessoas ou entidades autorizadas pelo proprietário da informação.

Comentários

Os quatro princípios considerados centrais ou principais, mais comumente cobrados em provas, estão listados na questão, a saber: a confidencialidade, a integridade, a disponibilidade e a autenticidade (É possível encontrar a sigla **CIDA**, ou **DICA**, para fazer menção a estes princípios!).

D	isponibilidade
I	ntegridade
C	onfidencialidade
A	utenticidade

Figura. Mnemônico **DICA**

É a confidencialidade (sigilo) que evitará o acesso não autorizado às informações, permitindo somente que *pessoas explicitamente autorizadas possam acessá-las.* A integridade evita alterações nos dados, *garantindo que a informação que foi armazenada é a que será recuperada*.

Gabarito: item errado.

9. **(CESPE/MPE-PI/Técnico Ministerial/Área: Administrativa/ 2012)** Worms são programas maliciosos que se autorreplicam em redes de computadores anexados a algum outro programa existente e instalado em computadores da rede.

Comentários

Os Worms (vermes) têm a capacidade de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Nesse caso, diferentemente do vírus, o Worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.

Gabarito: item errado.

10. **(CESPE/2002/POLÍCIA FEDERAL/PERITO: ÁREA 3 . COMPUTAÇÃO)** Sistemas criptográficos são ditos simétricos ou de chave secreta quando a chave utilizada para cifrar é a mesma utilizada para decifrar. Sistemas assimétricos ou de chave pública utilizam chaves distintas para cifrar e decifrar. Algoritmos simétricos são geralmente mais eficientes computacionalmente que os assimétricos e por isso são preferidos para cifrar grandes massas de dados ou para operações online.

Comentários

A **criptografia de chave simétrica** (também chamada de **criptografia de chave única**, ou **criptografia privada,** ou **criptografia convencional**) utiliza **APENAS UMA** chave para encriptar e decriptar as mensagens. Assim, como só utiliza UMA chave, obviamente ela deve ser compartilhada entre o remetente e o destinatário da mensagem.

Para ilustrar os sistemas simétricos, podemos usar a imagem de um cofre, que só pode ser fechado e aberto com uso de uma chave. Esta pode ser, por exemplo, uma combinação de números. A mesma combinação abre e fecha o cofre. Para criptografar uma mensagem, usamos a chave (fechamos o cofre) e para decifrá-la utilizamos a mesma chave (abrimos o cofre).

Os sistemas simétricos têm o problema em relação à distribuição de chaves, que devem ser combinadas entre as partes antes que a comunicação segura se inicie. Esta distribuição se torna um problema em situações em que as partes não podem se encontrar facilmente. Mas há outros problemas: a chave pode ser interceptada e/ou alterada em trânsito por um inimigo.

Na criptografia simétrica (ou de chave única) tanto o emissor quanto o receptor da mensagem devem conhecer a chave utilizada!!

Nos algoritmos de **criptografia assimétrica (criptografia de chave pública)** utilizam **DUAS** chaves **DIFERENTES**, uma **PÚBLICA** (que pode ser distribuída) e uma **PRIVADA** (pessoal e intransferível). Assim, nesse método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Do ponto de vista do custo computacional, **os sistemas simétricos apresentam melhor desempenho que os sistemas assimétricos**, e isso já foi cobrado em provas várias vezes!

Gabarito: item correto.

11. **(CESPE/Agente Técnico de Inteligência – Área de Tecnologia da Informação – ABIN/2010)** A chave assimétrica é composta por duas chaves criptográficas: uma privada e outra pública.

Comentários

A criptografia de chave pública (a*SS*imétrica) utiliza *duas* chaves: *uma* denominada *privada* e outra denominada *pública*. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave *pública*. Outra chave deve ser criada para a decodificação. Esta – a chave *privada* – é *secreta*.

Gabarito: item correto.

12. **(CESPE/Oficial Técnico de Inteligência-Área de Arquivologia - ABIN/2010)** A respeito de mecanismos de segurança da informação, e considerando que uma mensagem tenha sido criptografada com a chave pública de determinado destino e enviada por meio de um canal de comunicação, pode-se afirmar que a mensagem criptografada com a chave pública do destinatário garante que somente quem gerou a informação criptografada e o destinatário sejam capazes de abri-la.

Comentários

Quando se criptografa a mensagem com a chave pública do destinatário ela poderá ser aberta (descriptografada) apenas pelo destinatário, já que só ele tem acesso à sua chave privada. O remetente (quem gerou a mensagem) já tem acesso à mensagem em claro, não criptografada.

Gabarito: item errado.

Muita atenção aqui pessoal!!

Fique Atento!

Na **criptografia assimétrica** ou simplesmente **criptografia de chaves públicas**, as entidades envolvidas possuem duas chaves, uma privada e uma pública.

- **Quando a intenção é fazer uso da confidencialidade**, o emissor/remetente precisa conhecer a chave pública do destinatário/receptor, sendo assim, o emissor/remetente criptografa a mensagem utilizando a chave pública do destinatário/receptor, para descriptografar a mensagem o destinatário utiliza sua própria chave privada.
- **Quando se quer atestar a autenticidade**, o emissor/remetente precisa assinar o documento a ser transmitido, exemplo é assinatura digital, correio eletrônico, aplicações por meio do SSL, entre outros. O remetente/emissor criptografa o documento utilizando sua chave privada, e disponibiliza sua chave pública ao destinatário/receptor.

Outra aplicação para o uso de criptografias de chaves públicas são os certificados digitais. O certificado digital é

um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública.

13. **(CESPE/2010/Caixa/Técnico Bancário)** O destinatário de uma **mensagem assinada** utiliza a chave pública do remetente para garantir que essa mensagem tenha sido enviada pelo próprio remetente.

Comentários

Esta é uma das utilidades do uso de criptografia assimétrica. O emissor utiliza sua chave privada para encriptar a mensagem, sendo possível a decriptação apenas com sua chave pública. Assim, pode-se confirmar que o emissor é quem diz ser, pois somente a chave dele permite decriptar a mensagem.

Complementando, a questão refere-se ao princípio da **autenticidade** e é exatamente isso, a mensagem é criptografada com a chave privada do remetente, e é descriptografada pelo destinatário/receptor utilizando a chave pública do remetente/emissor.

Gabarito: item correto.

14. **(CESPE/2010/Caixa/Técnico Bancário)** A assinatura digital facilita a identificação de uma comunicação, pois baseia-se em criptografia simétrica de uma única chave.

Comentários

A assinatura digital facilita a identificação de uma comunicação, mas baseia-se em criptografia **assimétrica** com par de chaves: uma pública e outra privada.

Gabarito: item errado.

15. **(CESPE/TCU/Técnico Federal de Controle Externo/2012)** Por meio de certificados digitais, é possível assinar digitalmente documentos a fim de garantir o sigilo das informações contidas em tais documentos.

Comentários

A assinatura digital, por si só, não garante a confidencialidade (sigilo) dos dados, pois, teoricamente, todos possuem a chave pública do remetente. Essa confidencialidade é obtida por meio de técnicas de criptografia, que são utilizadas em conjunto com as assinaturas digitais!

A assinatura digital fornece uma prova inegável de que uma mensagem veio do emissor. Para verificar esse requisito, uma assinatura deve ter as seguintes propriedades:

- **autenticidade**: o receptor (destinatário de uma mensagem) pode confirmar que a assinatura foi feita pelo emissor;

- **integridade**: qualquer alteração da mensagem faz com que a assinatura seja invalidada;
- **não repúdio (irretratabilidade)**: o emissor (aquele que assinou digitalmente a mensagem) não pode negar que foi o autor da mensagem, ou seja, não pode dizer mais tarde que a sua assinatura foi falsificada.

Gabarito: item errado.

16. **(CESPE/AL-ES/Procurador/2011)** Caso o usuário acesse uma página na Internet e lhe seja apresentado um certificado digital válido, é correto inferir que a conexão utilizada por esse usuário estará cifrada com o uso de *pendrive.*

Comentários

A conexão utilizada estará cifrada com o uso do protocolo HTTPS (HyperText Transfer Protocol Secure - Protocolo de Transferência de Hipertexto Seguro). O HTTPS trata-se de uma variação do protocolo HTTP que utiliza mecanismos de segurança. Ele permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente. Diferentemente do HTTP (porta 80), a porta padrão usada pelo protocolo HTTPS é a porta **443**. Geralmente o HTTPS é utilizado para evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros. O endereço dos recursos na Internet que estão sob o protocolo HTTPS inicia-se por 'https://'. Um bom exemplo é o uso do HTTPS em sites de compras online.

Gabarito: item errado.

17. **(CESPE/Oficial Técnico de Inteligência/Área de Desenvolvimento e Manutenção de Sistemas – ABIN/2010)** As assinaturas digitais atuam sob o princípio básico da confidencialidade da informação, uma vez que conferem a autenticação da identidade do remetente de uma mensagem. No entanto, tal solução não garante a integridade da informação, que deve ser conferida por meio de tecnologias adicionais de criptografia.

Comentários

Com as assinaturas digitais temos garantida a autenticidade, a integridade e o não repúdio.

Gabarito: item errado.

18. **(CESPE/Técnico Bancário/Carreira administrativa- Caixa Econômica Federal-NM1/2010)** Para assinar uma mensagem digital, o remetente usa uma chave privada.

Comentários

O remetente usa *sua chave privada* para realizar um processo matemático com a mensagem, gerando caracteres de assinatura (chamamos aqui de "assinar a mensagem").

Gabarito: item correto.

19. **(CESPE/AL-ES/Cargos de Nível Médio/2011)** Existem diversos dispositivos que protegem tanto o acesso a um computador quanto a toda uma rede. Caso um usuário pretenda impedir que o tráfego com origem na Internet faça conexão com seu computador pessoal, a tecnologia adequada a ser utilizada nessa situação será o IpV6.

Comentários

IpV6 é a versão mais atual do protocolo IP. *O dispositivo a ser utilizado para* impedir que o tráfego com origem na Internet faça conexão com o computador pessoal do usuário é o Firewall, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Gabarito: item errado.

20. **(CESPE/Técnico Administrativo – Nível Médio – PREVIC/2011)** Firewall é o elemento de defesa mais externo na intranet de uma empresa e sua principal função é impedir que usuários da intranet acessem qualquer rede externa ligada à Web.

Comentários

O firewall tem como *principal* função impedir a entrada de usuários não autorizados e não impedir a saída (os usuários da intranet podem acessar sites na Internet, sem problemas), apesar de poder ser configurado dessa forma também!!

Gabarito: item errado.

21. **(CESPE/CBM-DF/Oficial Bombeiro Militar Complementar/Informática/2011)** Em uma VPN (*virtual private network*) que utilize a técnica de tunelamento, os conteúdos dos pacotes que trafegam pela Internet são criptografados, ao passo que, para permitir o roteamento eficiente dos pacotes, os seus endereços de origem e de destino permanecem não criptografados.

Comentários

Na técnica de tunelamento, os dados e endereços estão em um único pacote de dados, que está criptografado. Assim, todo o conteúdo do pacote é criptografado, inclusive os endereços de origem e de destino.

Gabarito: item errado.

22. **(CESPE/MPE-PI/2012)** A adoção de crachás para identificar as pessoas e controlar seus acessos às dependências de uma empresa é um mecanismo adequado para preservar a segurança da informação da empresa.

Comentários

Essa é uma das medidas necessárias para resguardar a segurança na empresa.

Gabarito: item correto.

23. **(CESPE/Nível Superior - PREVIC/2011)** Por meio do uso de certificados digitais, é possível garantir a integridade dos dados que transitam pela Internet, pois esses certificados são uma forma confiável de se conhecer a origem dos dados.

Comentários

Integridade não tem relação com a origem dos dados. Integridade diz respeito à não alteração dos dados. Conhecer a origem está ligado ao princípio da autenticidade.

Gabarito: item errado.

24. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** Tecnologias como a biometria por meio do reconhecimento de digitais de dedos das mãos ou o reconhecimento da íris ocular são exemplos de aplicações que permitem exclusivamente garantir a integridade de informações.

Comentários

A ***biometria*** está sendo cada vez mais utilizada na segurança da informação, permitindo a utilização de características corporais, tais como: *impressões digitais, timbre de voz, mapa da íris, análise geométrica da mão, etc.,* em mecanismos de autenticação. O princípio da integridade destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, e teremos outros mecanismos na organização para mantê-la. A biometria, no entanto, garante-nos a autenticidade, relacionada à capacidade de garantir a identidade de uma pessoa (física ou jurídica) que acessa as

informações do sistema ou de um servidor (computador).
Gabarito: item errado.

25. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** Um filtro de phishing é uma ferramenta que permite criptografar uma mensagem de email cujo teor, supostamente, só poderá ser lido pelo destinatário dessa mensagem.

Comentários

O filtro de phishing ajuda a protegê-lo contra fraudes e riscos de furto de dados pessoais, mas a ferramenta não permite criptografar mensagens!

Gabarito: item errado.

26. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** O conceito de confidencialidade refere-se a disponibilizar informações em ambientes digitais apenas a pessoas para as quais elas foram destinadas, garantindo-se, assim, o sigilo da comunicação ou a exclusividade de sua divulgação apenas aos usuários autorizados.

Comentários

A confidencialidade é a garantia de que a informação não será conhecida por quem não deve, ou seja, somente pessoas explicitamente autorizadas poderão acessá-las.

Gabarito: item correto.

27. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** É necessário sempre que o software de antivírus instalado no computador esteja atualizado e ativo, de forma a se evitar que, ao se instalar um cookie no computador do usuário, essa máquina fique, automaticamente, acessível a um usuário intruso (hacker), que poderá invadi-la.

Comentários

Recomenda-se que o antivírus esteja sempre atualizado e ativo no computador do usuário. No entanto, um cookie não permite que a máquina seja acessível por um intruso, pois se trata de um arquivo texto que o servidor Web salva na máquina do usuário para armazenar as suas preferências de navegação, dentre outros.

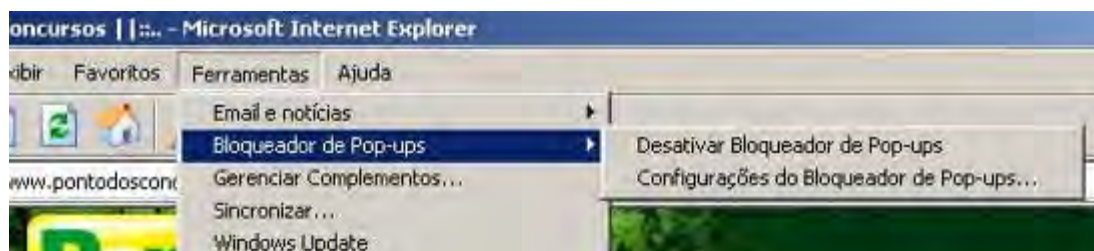
Gabarito: item errado.

28. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** Os pop-ups são vírus que podem ser eliminados pelo chamado bloqueador de pop-ups, se este estiver instalado na máquina. O bloqueador busca impedir, por exemplo,

que esse tipo de vírus entre na máquina do usuário no momento em que ele consultar um sítio da Internet.

Comentários

Pop-Up não é vírus, trata-se de uma janela aberta sobre a janela principal de um site, mostrando uma propaganda ou aviso sobre um determinado tema.

O bloqueador de pop-ups pode ser habilitado no menu Ferramentas -> Bloqueador de Pop-ups do Internet Explorer.

Gabarito: item errado.

29. **(CESPE/Técnico Administrativo - MPU/2010)** De acordo com o princípio da disponibilidade, a informação só pode estar disponível para os usuários aos quais ela é destinada, ou seja, não pode haver acesso ou alteração dos dados por parte de outros usuários que não sejam os destinatários da informação.

Comentários

Nesta questão houve uma confusão de conceitos. A segurança da informação está envolta por três princípios básicos: **C**onfidencialidade, **I**ntegridade e **D**isponibilidade. A disponibilidade, como o nome sugere, refere-se à garantia de que a informação estará disponível quando dela se quiser fazer uso. Naturalmente a informação deve estar disponível a quem de direito, como manda o princípio da confidencialidade. Quem garante o sigilo da informação é este último princípio, enquanto o princípio que garante que a informação está intacta (que não possui modificações não autorizadas) é o princípio da integridade. Esta é a tríade **CID –** *Confidencialidade, Integridade e Disponibilidade*. Observe o quadro a seguir:

Princípio básico	*Conceito*	*Objetivo*
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.	Proteger contra o acesso não autorizado, mesmo para dados em trânsito.

Integridade	Propriedade de salvaguarda da exatidão e completeza de ativos.	Proteger informação contra modificação sem permissão; garantir a fidedignidade das informações.
Disponibilidade	Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.	Proteger contra indisponibilidade dos serviços (ou degradação); Garantir aos usuários com autorização, o acesso aos dados.

Gabarito: item errado.

30. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** Confidencialidade, disponibilidade e integridade da informação, que são conceitos importantes de segurança da informação em ambiente digital, devem estar presentes na gestão e no uso de sistemas de informação, em benefício dos cidadãos e dos fornecedores de soluções.

Comentários

Os princípios da segurança da informação listados na questão são:

- **C**onfidencialidade**:** a garantia de que a informação não será conhecida por quem não deve, ou seja, somente pessoas explicitamente autorizadas poderão acessá-las;
- **I**ntegridade**:** destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais ou acidentais.
- **D**isponibilidade**:** é a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo;

Cabe ressaltar que a perda de pelo menos um desses princípios já irá comprometer o ambiente da empresa, portanto devem estar presentes na gestão e no uso de sistemas de informação, em benefício dos cidadãos e dos fornecedores de soluções.

Gabarito: item correto.

31. **(CESPE/Nível Superior - STM/2011)** Um firewall pessoal instalado no computador do usuário impede que sua máquina seja infectada por qualquer tipo de vírus de computador.

Comentários

O Firewall não protege contra infecção de vírus e sim contra o acesso não autorizado (invasões), quem protege contra infecção de vírus é o Antivírus.

Gabarito: item errado.

32. **(CESPE/Analista Judiciário - Tecnologia da Informação-TRE-MT/2010)** A confidencialidade tem a ver com salvaguardar a exatidão e a inteireza das informações e métodos de processamento. Para tanto, é necessário que os processos de gestão de riscos identifiquem, controlem, minimizem ou eliminem os riscos de segurança que podem afetar sistemas de informações, a um custo aceitável.

Comentários

Primeiro, a confidencialidade é a garantia de segredo. A afirmação fala da Integridade. Outra coisa é que não se fala em ELIMINAR riscos e sim minimizar.

Gabarito: item errado.

33. **(CESPE/ANALISTA- TRE.BA/2010)** Confidencialidade, disponibilidade e integridade da informação são princípios básicos que orientam a definição de políticas de uso dos ambientes computacionais. Esses princípios são aplicados exclusivamente às tecnologias de informação, pois não podem ser seguidos por seres humanos.

Comentários

Os seres humanos também são considerados como ativos em segurança da informação e merecem também uma atenção especial por parte das organizações. Aliás, os usuários de uma organização são considerados até como o "elo mais fraco da segurança", e são os mais vulneráveis. Portanto, eles têm que seguir as regras predefinidas pela política de segurança da organização, e estão sujeitos a punições para os casos de descumprimento das mesmas! Não adianta investir recursos financeiros somente em tecnologias e esquecer de treinar os usuários da organização, pois erros comuns (como o uso de um *pen drive* contaminado por vírus na rede) poderiam vir a comprometer o ambiente que se quer proteger!

Gabarito: item errado.

34. **(CESPE/Analista de Saneamento/Analista de Tecnologia da Informação – Desenvolvimento - EMBASA/2010)** O princípio da autenticação em segurança diz que um usuário ou processo deve ser corretamente identificado. Além disso, todo processo ou usuário autêntico está automaticamente autorizado para uso dos sistemas.

Comentários

Cuidado aqui! A segunda parte da afirmação está incorreta. Um usuário ou processo (programa) autenticado não está automaticamente apto para uso dos sistemas. Isto dependerá do nível de acesso que ele possuir. É possível, por exemplo, que um usuário tenha permissão apenas para visualizar a caixa de mensagens dele ou, ainda, para ler os arquivos de sua pasta particular.

Gabarito: item errado.

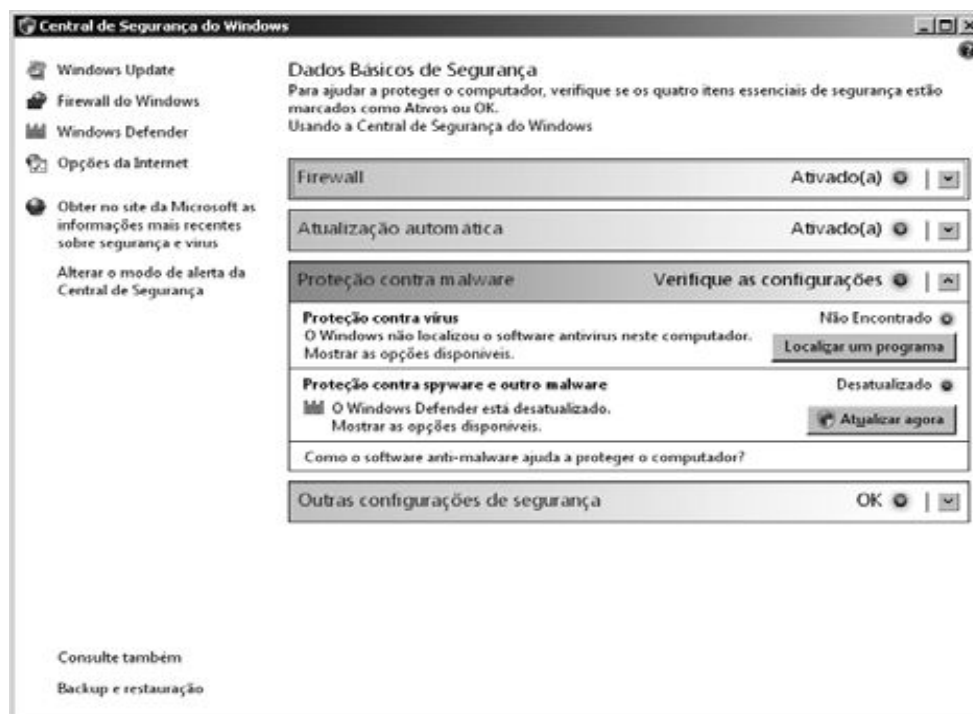
35. **(CESPE/Técnico Administrativo - ANATEL/2009)** Com o desenvolvimento da Internet e a migração de um grande número de sistemas especializados de informação de grandes organizações para sistemas de propósito geral acessíveis universalmente, surgiu a preocupação com a segurança das informações no ambiente da Internet. Acerca da segurança e da tecnologia da informação, julgue o item a seguir.

    -> A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los.

Comentários

O conceito de disponibilidade está correto, mas o conceito de integridade não. O conceito apresentado na questão foi o de confidencialidade: "garantia de que sistemas de informações sejam *acessíveis apenas àqueles autorizados* a acessá-los".

Gabarito: item errado.

(CESPE/Escrivão de Polícia Federal/2010)

Considerando a figura acima, que apresenta uma janela com algumas informações da central de segurança do Windows de um sistema computacional (host) de uso pessoal ou corporativo, julgue os três próximos itens, a respeito de segurança da informação.

36. **(CESPE/2010/Escrivão de Polícia Federal)** A atualização automática disponibilizada na janela exibida acima é uma função que está mais relacionada à distribuição de novas funções de segurança para o sistema operacional do que à distribuição de novos patches (remendos) que corrijam as vulnerabilidades de código presentes no sistema operacional.

Comentários

A atualização automática disponibilizada na janela está relacionada à distribuição de novos patches (remendos/correções de segurança) que corrijam as vulnerabilidades (fragilidades) de código presentes no sistema operacional.

Gabarito: item errado.

37. **(CESPE/2010/Escrivão de Polícia Federal)** Na figura anterior, o firewall assinalado como ativado, em sua configuração padrão, possui um conjunto maior de regras para bloqueio de conexões originadas de fora do computador do que para as conexões originadas de dentro do computador.

Comentários

Cumpre a função de controlar os acessos. Uma vez estabelecidas suas regras, passam a gerenciar tudo o que deve entrar e sair da rede corporativa, tendo

um conjunto maior de regras para bloqueio de conexões oriundas de fora do computador.

Gabarito: item correto.

38. **(CESPE/2010/Escrivão de Polícia Federal)** A configuração da proteção contra malwares exposta na figura indica que existe no host uma base de assinaturas de vírus instalada na máquina.

Comentários

A figura destaca que não existe antivírus instalado no equipamento, e também mostra que a proteção contra spyware e outro malware encontra-se desatualizada. Não é possível destacar pela figura que existe no host (equipamento) uma base de assinaturas de vírus.

Gabarito: item errado.

39. (CESPE/2010/Caixa/Técnico Bancário/Administrativo) Uma autoridade de registro emite o par de chaves do usuário que podem ser utilizadas tanto para criptografia como para assinatura de mensagens eletrônicas.

Comentários

É a autoridade de registro recebe as solicitações de certificados dos usuários e as envia à autoridade certificadora que os emite.

Gabarito: item errado.

Atenção aqui!!

Componentes de uma ICP

Uma Infraestrutura de Chaves Públicas (ICP) envolve um processo colaborativo entre várias entidades: autoridade certificadora (AC), autoridade de registro (AR), repositório de certificados e o usuário final.

Autoridade Certificadora (AC)

Vamos ao exemplo da carteira de motorista. Se pensarmos em um certificado como uma carteira de motorista, a Autoridade Certificadora opera como um tipo de órgão de licenciamento. Em uma ICP, a AC emite, gerencia e revoga os certificados para uma comunidade de usuários finais. A AC assume a tarefa de autenticação de seus usuários finais e então assina digitalmente as informações sobre o certificado

antes de disseminá-lo. A AC, no final, é responsável pela autenticidade dos certificados emitidos por ela.

Autoridade de Registro (AR)

Embora a AR possa ser considerada um componente estendido de uma ICP, os administradores estão descobrindo que isso é uma necessidade. À medida que aumenta o número de usuários finais dentro de uma ICP, também aumenta a carga de trabalho de uma AC.

A AR serve como uma entidade intermediária entre a AC e seus usuários finais, ajudando a AC em suas funções rotineiras para o processamento de certificados.

Uma AR é necessariamente uma entidade operacionalmente vinculada a uma AC, a quem compete:

- identificar os titulares de certificados: indivíduos, organizações ou equipamentos;
- encaminhar solicitações de emissão e revogação de certificados à AC;
- guardar os documentos apresentados para identificação dos titulares.

A AC deve manter uma lista de suas ARs credenciadas e estas ARs são consideradas confiáveis, pelo ponto de vista dessa AC.

Resumindo...

a AC emite, gerencia e revoga os certificados para uma comunidade de usuários finais. A AR serve como uma entidade intermediária entre a AC e seus usuários finais, ajudando a AC em suas funções rotineiras para o processamento de certificados.

40. **(CESPE/Técnico Judiciário/Programação de Sistemas - TRE-MT/2010)** Disponibilidade é a garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas.

Comentários

A disponibilidade garante que a informação estará lá quando for preciso acessá-la. Obviamente, o acesso só será permitido a quem de direito. O texto da questão afirma que a disponibilidade é a garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas, o que é a garantia da confidencialidade.

Gabarito: item errado.

41. **(CESPE/TRE-MT/Técnico Judiciário - Programação de Sistemas/2010)** Confidencialidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Comentários

O texto refere-se à disponibilidade. A informação deve estar disponível a quem de direito.

Gabarito: item errado.

42. (CESPE/UERN/Agente Técnico Administrativo/2010) A disponibilidade da informação é a garantia de que a informação não será alterada durante o trânsito entre o emissor e o receptor, além da garantia de que ela estará disponível para uso nesse trânsito.

Comentários

Nem uma coisa nem outra. A disponibilidade garante que a informação estará disponível aos usuários com direito de acesso quando for preciso, mas no local apropriado para o armazenamento.

Gabarito: item errado.

43. **(CESPE/AGU/Contador/2010)** Um arquivo criptografado fica protegido contra contaminação por vírus.

Comentários

O arquivo criptografado não elimina a possibilidade de infecção por vírus. Lembre-se de que a criptografia modifica os símbolos do texto, mas não impede a inclusão de vírus na sequência.

Gabarito: item errado.

44. (CESPE/UERN/Agente Técnico Administrativo/2010) Cavalo de troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.

Comentários

O *Trojan Horse* (Cavalo de Troia) pode utilizar um mecanismo de propagação bastante eficiente, escondendo-se dentro de um aplicativo útil.

Gabarito: item correto.

45. **(CESPE/UERN/Agente Técnico Administrativo/2010)** O uso de um programa anti-spam garante que software invasor ou usuário mal-intencionado não acesse uma máquina conectada a uma rede.

Comentários

Anti-spam refere-se aos e-mails indesejados apenas. É um software que filtra os e-mails recebidos separando os não desejados.

Gabarito: item errado.

46. **(CESPE/SEDU-ES/Agente de Suporte Educacional/2010)** Vírus é um programa que pode se reproduzir anexando seu código a um outro programa, da mesma forma que os vírus biológicos se reproduzem.

Comentários

Os vírus são pequenos códigos de programação maliciosos que se "agregam" a arquivos e são transmitidos com eles. Quando o arquivo é aberto na memória RAM, o vírus também é, e, a partir daí se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. Assim, do mesmo modo como um vírus biológico precisa de material reprodutivo das células hospedeiras para se copiar, o vírus de computador necessita de um ambiente propício para sua existência... Esse ambiente é o arquivo a quem ele (o vírus) se anexa.

Gabarito: item correto.

47. **(CESPE/SEDU-ES/Agente de Suporte Educacional/2010)** Cavalos-de-troia, adwares e vermes são exemplos de pragas virtuais.

Comentários

Todos os três programas mencionados são exemplos de pragas virtuais, conforme visto a seguir:

- O Cavalo de Troia é um programa no qual um código malicioso ou prejudicial está contido dentro de uma programação ou dados aparentemente inofensivos de modo a poder obter o controle e causar danos.
- ***Adware*** **(*Advertising software*)** é um software projetado para exibir anúncios de propaganda em seu computador. Esses softwares podem ser maliciosos!

- ***Worms***: são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os *worms* apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!!).

Gabarito: item correto.

48. **(CESPE/SEDU-ES/AGENTE DE SUPORTE EDUCACIONAL/2010)** Backup é o termo utilizado para definir uma cópia duplicada de um arquivo, um disco, ou um dado, feita com o objetivo de evitar a perda definitiva de arquivos importantes.

Comentários

O termo *backup* (cópia de segurança) está relacionado às cópias feitas de um arquivo ou de um documento, de um disco, ou um dado, que deverão ser guardadas sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo, de maneira a permitir o resgate de programas ou informações importantes em caso de falha ou perda dos originais.

Gabarito: item correto.

49. **(CESPE/EMBASA/Analista de Saneamento - Analista de TI – Área: Desenvolvimento/2010)** O princípio da autenticação em segurança diz que um usuário ou processo deve ser corretamente identificado. Além disso, todo processo ou usuário autêntico está automaticamente autorizado para uso dos sistemas.

Comentários

É por meio da autenticação que se confirma a identidade do usuário ou processo (programa) que presta ou acessa as informações. No entanto, afirmar que TODO processo ou usuário autêntico está automaticamente autorizado é falsa, já que essa autorização dependerá do nível de acesso que ele possui. Em linhas gerais, **autenticação** é o processo de provar que você é quem diz ser. **Autorização** é o processo de determinar o que é permitido que você faça depois que você foi autenticado!!

Gabarito: item errado.

50. **(CESPE/TRE-MT/Analista Judiciário - Tecnologia da Informação/2010)** Uma das vantagens da criptografia simétrica em relação à assimétrica é a maior velocidade de cifragem ou decifragem das mensagens. Embora os algoritmos de chave assimétrica sejam mais rápidos

que os de chave simétrica, uma das desvantagens desse tipo de criptografia é a exigência de uma chave secreta compartilhada.

Comentários

Inverteu os conceitos. Os algoritmos mais rápidos e que compartilham chaves são os algoritmos de chave simétrica.

Gabarito: item errado.

51. (CESPE/TRE-MT/Analista Judiciário/Tecnologia da Informação/2010) Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é privada e divulgada para o transmissor, enquanto a chave usada para decriptar a mensagem é pública.

Comentários

O erro está na localização das palavras pública e privada. Devem ser trocadas de lugar. A chave utilizada para encriptar a mensagem é **pública** e divulgada para o transmissor, enquanto a chave usada para decriptar a mensagem é **privada.**

Gabarito: item errado.

52. **(CESPE/CAIXA-NM1/ Técnico Bancário/Carreira administrativa/2010)** Autoridade certificadora é a denominação de usuário que tem poderes de acesso às informações contidas em uma mensagem assinada, privada e certificada.

Comentários

Autoridade certificadora (AC) é o termo utilizado para designar a entidade que emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Além disso, emite e publica a LCR (Lista de Certificados Revogados).

Gabarito: item errado.

53. **(CESPE/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA/2010)** A autoridade reguladora tem a função de emitir certificados digitais, funcionando como um cartório da Internet.

Comentários

A Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais.

Gabarito: item errado.

54. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** O ITI (Instituto Nacional de Tecnologia da Informação) é também conhecido como Autoridade Certificadora Raiz Brasileira.

Comentários

A **Autoridade Certificadora RAIZ** (**AC Raiz)** é primeira autoridade da cadeia de certificação e compete a ela **emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente**, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de **fiscalização e auditoria das AC's e das AR's e dos prestadores de serviço habilitados na ICP**. A função da AC-Raiz foi delegada ao **Instituto Nacional de Tecnologia da Informação – ITI,** autarquia federal atualmente ligada à Casa Civil da Presidência da República. Logo, o ITI é também conhecido como Autoridade Certificadora Raiz Brasileira. A AC-Raiz só pode emitir certificados às AC's imediatamente subordinadas, sendo vedada de emitir certificados a usuários finais.

Gabarito: item correto.

55. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** PKI ou ICP é o nome dado ao certificado que foi emitido por uma autoridade certificadora.

Comentários

PKI (***Public Key Infrastrusture***) é a infraestrutura de chaves públicas. A ICP-Brasil é um exemplo de PKI.

Gabarito: item errado.

56. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** Um certificado digital é pessoal, intransferível e não possui data de validade.

Comentários

Um certificado digital é um **documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores**

(computadores) dentre outras entidades. Este “documento” na verdade é uma **estrutura de dados** que contém a chave pública do seu titular e outras informações de interesse. Contêm informações relevantes para a identificação ”real” da entidade a que visam certificar (CPF, CNPJ, endereço, nome, etc) e informações relevantes para a aplicação a que se destinam. O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação. Chamamos essa autoridade de Autoridade Certificadora, ou AC. Dentre as informações que compõem um certificado temos:

- **Versão:** indica qual formato de certificado está sendo seguido
- **Número de série:** identifica unicamente um certificado dentro do escopo do seu emissor.
- **Algoritmo:** identificador dos algoritmos de hash+assinatura utilizados pelo emissor para assinar o certificado.
- **Emissor:** entidade que emitiu o certificado.
- **Validade:** data de emissão e expiração.
- **Titular:** nome da pessoa, URL ou demais informações que estão sendo certificadas.
- **Chave pública:** informações da chave pública do titular.
- **Extensões:** campo opcional para estender o certificado.
- **Assinatura:** valor da assinatura digital feita pelo emissor.

Gabarito: item errado.

57. **(CESPE/2010/UERN/TÉCNICO DE NÍVEL SUPERIOR-Adaptada)** Vírus, worms e cavalos-de-troia são exemplos de software mal-intencionados que têm o objetivo de, deliberadamente, prejudicar o funcionamento do computador. O firewall é um tipo de malware que ajuda a proteger o computador contra cavalos-de-troia.

Comentários

Os vírus, *worms* e cavalos-de-troia são exemplos de software mal-intencionados que têm o objetivo de, deliberadamente, prejudicar o funcionamento do computador, e, consequentemente, o usuário!! O cavalo de troia por exemplo "parece" ser inofensivo, quando na verdade não é!! É um presente de grego (rs)!! Fica instalado no seu computador abrindo portas para que a máquina seja acessada remotamente, pode funcionar como um keylogger ao capturar as informações digitadas no computador, etc, portanto, a primeira parte da assertiva está correta.

A assertiva tornou-se falsa ao afirmar que o *firewall* é um tipo de *malware*, um absurdo! O *malware* (*malicious software*) é um software destinado a se infiltrar em um sistema de computador de forma ilícita, com o intuito de causar

algum dano ou roubo de informações (confidenciais ou não), e não é esse o objetivo do *firewall*.

Gabarito: item errado.

58. **(CESPE/2010/UERN/Agente Técnico Administrativo)** Uma das formas de se garantir a segurança das informações de um website é não colocá-lo em rede, o que elimina a possibilidade de acesso por pessoas intrusas.

Comentários

Colocar um site fora da rede significa que ninguém terá acesso via rede ao site, nem mesmo as pessoas autorizadas. Além disso, não se esqueça dos acessos feitos localmente, direto na máquina onde o site está hospedado!

Gabarito: item errado.

59. **(CESPE/2010/TRE-MT/Analista Judiciário - Tecnologia da Informação)** A segurança física objetiva impedir acesso não autorizado, danos ou interferência às instalações físicas e às informações da organização. A proteção fornecida deve ser compatível com os riscos identificados, assegurando a preservação da confidencialidade da informação.

Comentários

Não esquecer que além da proteção lógica, deve existir a proteção física. De nada adianta um sistema protegido dos acessos não autorizados via rede se é permitido o acesso físico à máquina. Um atacante pode incendiar, quebrar, estragar, roubar e até invadir um sistema quando o mesmo não possui controles físicos.

Gabarito: item correto.

60. **(CESPE/2010/TRE-MT/Analista Judiciário - Tecnologia da Informação)** Serviços de não repudiação são técnicas utilizadas para detectar alterações não autorizadas ou corrompimento dos conteúdos de uma mensagem transmitida eletronicamente. Essas técnicas, que têm como base o uso de criptografia e assinatura digital, podem ajudar a estabelecer provas para substanciar se determinado evento ou ação ocorreu.

Comentários

Não repúdio ocorre quando não é possível ao emissor da mensagem negar a autoria da mesma.

Gabarito: item errado.

61. **(CESPE/2010/EMBASA/ANALISTA DE SANEAMENTO)** Um firewall em uma rede é considerado uma defesa de perímetro e consegue coibir todo tipo de invasão em redes de computadores.

Comentários

O firewall, como o nome sugere (traduzindo = parede de fogo) é uma barreira tecnológica entre dois pontos de uma rede, em que normalmente é o único ponto de acesso entre a rede interna e a Internet. O firewall deverá permitir somente a passagem de tráfego autorizado. Além disso, tem a função de filtrar todo o tráfego de rede que passa por ele, dizendo o que é permitido e o que é bloqueado ou rejeitado.

Pode ser comparado com uma sequência de perguntas e respostas. Por exemplo, o firewall faz uma pergunta ao pacote de rede, se a resposta for correta ele deixa passar o tráfego ou encaminha a requisição a outro equipamento, se a resposta for errada ele não permite a passagem ou então rejeita o pacote. O firewall não consegue coibir todos os tipos de invasão.

Um firewall qualquer nunca vai proteger uma rede de seus usuários internos, independente da arquitetura, tipo, sistema operacional ou desenvolvedor, pois os usuários podem manipular os dados dentro das corporações das formas mais variadas possíveis, como exemplo, se utilizando de um pen drive, para roubar ou passar alguma informação para um terceiro ou até mesmo para uso próprio.

Um firewall nunca irá proteger contra serviços ou ameaças totalmente novas, ou seja, se hoje surgir um novo tipo de ataque *spoofing*, não necessariamente esse firewall vai proteger desse tipo de ataque, pois é uma nova técnica existente no mercado e até o final de sua implementação, não se tinha conhecimento sobre a mesma, o que acarreta na espera de uma nova versão que supra essa necessidade.

Um firewall também não irá proteger contra vírus, pois os vírus são pacotes de dados como outros quaisquer. Para identificar um vírus é necessária uma análise mais criteriosa, que é onde o antivírus atua.

Gabarito: item errado.

62. **(CESPE/2009/TRE/PR/Técnico Judiciário – Especialidade: Operação de computadores)** Firewalls são equipamentos típicos do perímetro de segurança de uma rede, sendo responsáveis pela detecção e contenção de ataques e intrusões.

Comentários

Os firewalls são equipamentos típicos do perímetro de segurança de uma rede, no entanto é o **IPS** (Sistema de Prevenção de Intrusão) que faz a detecção de ataques e intrusões, e não o *firewall*!!

O firewall permite restringir o tráfego de comunicação de dados entre a parte da rede que está "dentro" ou "antes" do firewall, protegendo-a assim das ameaças da rede de computadores que está "fora" ou depois do firewall. Esse mecanismo de proteção geralmente é utilizado para proteger uma rede menor (como os computadores de uma empresa) de uma rede maior (como a Internet).

Gabarito: item errado.

63. **(CESPE/2008/TRT-1ªR/Analista Judiciário-Adaptada)** Uma característica das redes do tipo VPN (*virtual private networks*) é que elas nunca devem usar criptografia, devido a requisitos de segurança e confidencialidade.

Comentários

Uma **VPN** (***Virtual Private Network*** **– Rede Privada Virtual**) é uma rede **privada** (não é de acesso público!) que usa a estrutura de uma rede pública (como por exemplo, a **Internet**) para transferir seus dados (os dados devem estar **criptografados** para passarem despercebidos e inacessíveis pela Internet). As VPNs são muito utilizadas para interligar filiais de uma mesma empresa, ou fornecedores com seus clientes (em negócios eletrônicos) através da estrutura física de uma rede pública.

O tráfego de dados é levado pela rede pública utilizando protocolos <u>não necessariamente seguros</u>. **VPNs seguras usam protocolos de criptografia por tunelamento** que fornecem a confidencialidade (sigilo), autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Gabarito: item errado.

64. **(CESPE/2010/MINISTÉRIO DA SAÚDE /ANALISTA TÉCNICO-ADMINISTRATIVO)** Firewall é o mecanismo usado em redes de computadores para controlar e autorizar o tráfego de informações, por meio do uso de filtros que são configurados de acordo com as políticas de segurança estabelecidas.

Comentários

A banca especificou corretamente o conceito para o termo *firewall*. Em outras palavras, basicamente, o *firewall* é um sistema para controlar o acesso às redes de computadores, e foi desenvolvido para evitar acessos não autorizados em uma rede local ou rede privada de uma corporação.

Um *firewall* deve ser instalado no ponto de conexão entre as redes, onde, através de regras de segurança, controla o tráfego que flui para dentro e para fora da rede protegida.

Deve-se observar que isso o torna um potencial gargalo para o tráfego de dados e, caso não seja dimensionado corretamente, poderá causar atrasos e diminuir a *performance* da rede.

Gabarito: item correto.

65. **(CESPE/2010/TRE.BA/ANALISTA/Q.27)** Firewall é um recurso utilizado para a segurança tanto de estações de trabalho como de servidores ou de toda uma rede de comunicação de dados. Esse recurso possibilita o bloqueio de acessos indevidos a partir de regras preestabelecidas.

Comentários

Outra questão bem parecida com a anterior, que destaca claramente o conceito de *firewall*! Vários objetivos para a segurança de uma rede de computadores podem ser atingidos com a utilização de *firewalls*. Dentre eles destacam-se:

- segurança: evitar que usuários externos, vindos da Internet, tenham acesso a recursos disponíveis apenas aos funcionários da empresa autorizados. Com o uso de *firewalls* de aplicação, pode-se definir que tipo de informação os usuários da Internet poderão acessar (somente servidor de páginas e correio eletrônico, quando hospedados internamente na empresa);
- confidencialidade: pode ocorrer que empresas tenham informações sigilosas veiculadas publicamente ou vendidas a concorrentes, como planos de ação, metas organizacionais, entre outros. A utilização de sistemas de *firewall* de aplicação permite que esses riscos sejam minimizados;
- produtividade: é comum os usuários de redes de uma corporação acessarem *sites* na Internet que sejam improdutivos como *sites* de pornografia, piadas, chat etc. O uso combinado de um *firewall* de aplicação e um *firewall* de rede pode evitar essa perda de produtividade;
- *performance*: o acesso à Internet pode tornar-se lento em função do uso inadequado dos recursos. Pode-se obter melhoria de velocidade de acesso a Internet mediante controle de quais *sites* podem ser visitados, quem pode visitá-los e em que horários serão permitidos. A opção de geração de relatórios de acesso pode servir como recurso para análise dos acessos.

Gabarito: item correto.

66. **(CESPE/2010/UERN/TÉCNICO DE NÍVEL SUPERIOR-Adaptada)** Firewall é um sistema constituído de software e hardware que verifica informações oriundas da Internet ou de uma rede de computadores e que permite ou bloqueia a entrada dessas informações, estabelecendo, dessa

forma, um meio de proteger o computador de acesso indevido ou indesejado.

Comentários

O *firewall pode ser formado por um conjunto complexo de equipamentos e softwares, ou somente baseado em software*, o que já tornaria incorreta a questão, no entanto, a banca optou pela anulação da questão.

A função do *firewall* é **controlar o tráfego** entre duas ou mais redes, com o objetivo de fornecer segurança, prevenir ou reduzir ataques ou invasões às bases de dados corporativas, a uma (ou algumas) das redes, que normalmente têm informações e recursos que não devem estar disponíveis aos usuários da(s) outra(s) rede(s). Complementando, não são todas as informações oriundas da Internet ou de uma rede de computadores que serão bloqueadas, *ele realiza a filtragem dos pacotes e, então, bloqueia SOMENTE as transmissões NÃO PERMITIDAS*!

Gabarito: item anulado.

67. **(CESPE/2010/TRE-BA/Técnico Judiciário - Área Administrativa)** Uma das formas de bloquear o acesso a locais não autorizados e restringir acessos a uma rede de computadores é por meio da instalação de firewall, o qual pode ser instalado na rede como um todo, ou apenas em servidores ou nas estações de trabalho.

Comentários

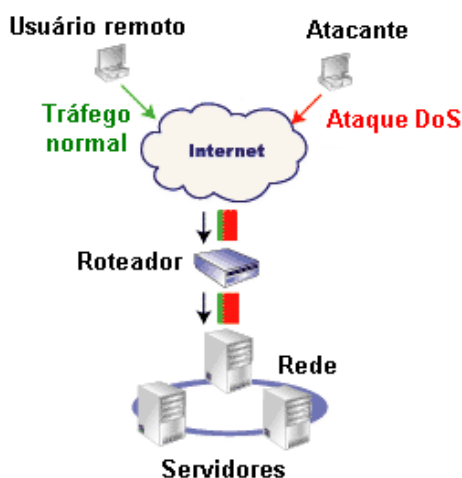
O firewall é uma das ferramentas da segurança da informação, que interage com os usuários de forma transparente, permitindo ou não o tráfego da rede interna para a Internet, como da Internet para o acesso a qualquer serviço que se encontre na rede interna da corporação e/ou instituição. Desta forma todo o tráfego, tanto de entrada como de saída em uma rede, deve passar por este "controlador" que aplica de forma implícita algumas das políticas de segurança adotadas pela corporação.

Gabarito: item correto.

68. **(CESPE/2004/POLÍCIA FEDERAL/REGIONAL/PERITO/ÁREA 3/Q. 105)** Um dos mais conhecidos ataques a um computador conectado a uma rede é o de negação de serviço (DoS – *denial of service*), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.

Comentários

No ataque de **Negação de Serviço (*Denial of Service - DoS*)** o atacante utiliza **um computador**, a partir do qual ele envia vários pacotes ou requisições de serviço de uma vez, para tirar de operação um serviço ou computador(es) conectado(s) à Internet, causando prejuízos. Para isso, são usadas técnicas que podem:

- gerar uma sobrecarga no processamento de um computador, de modo que o verdadeiro usuário do equipamento não consiga utilizá-lo;
- gerar um grande tráfego de dados para uma rede, ocasionando a indisponibilidade dela;
- indisponibilizar serviços importantes de um provedor, impossibilitando o acesso de seus usuários etc.

Gabarito: item correto.

69. **(CESPE/2008/PRF/Policial Rodoviário Federal)** O uso de firewall e de software antivírus é a única forma eficiente atualmente de se implementar os denominados filtros anti-spam.

Comentários

Para se proteger dos *spams* temos que instalar um *anti-spam*, uma nova medida de segurança que pode ser implementada independentemente do antivírus e do *firewall*.

O uso de um *firewall* (filtro que controla as comunicações que passam de uma rede para outra e, em função do resultado permite ou bloqueia seu passo), software antivírus e filtros *anti-spam* são mecanismos de segurança importantes.

Gabarito: item errado.

70. **(CESPE/2008/PRF-POLICIAL RODOVIÁRIO FEDERAL-ADAPTADA)** *Phishing* e *pharming* são pragas virtuais variantes dos denominados

cavalos-de-tróia, se diferenciando destes por precisarem de arquivos específicos para se replicar e contaminar um computador e se diferenciando, entre eles, pelo fato de que um atua em mensagens de e-mail trocadas por serviços de webmail e o outro, não.

Comentários

O ***Phishing*** (ou *Phishing scam*) e o **Pharming** (ou *DNS Poisoining*) não são pragas virtuais. *Phishing* e *Pharming* são dois tipos de golpes na Internet, e, portanto, não são variações de um cavalo de troia (*trojan horse*) – que se trata de um programa aparentemente inofensivo que entra em seu computador na forma de cartão virtual, álbum de fotos, protetor de tela, jogo etc, e que, quando executado (com a sua autorização!), parece lhe divertir, mas, por trás abre portas de comunicação do seu computador para que ele possa ser invadido.

Normalmente consiste em um único arquivo que necessita ser explicitamente executado. Para evitar a invasão, fechando as portas que o cavalo de troia abre, é necessário ter, em seu sistema, um programa chamado firewall.

Gabarito: item errado.

71. **(CESPE/2008/PRF/Policial Rodoviário Federal)** Se o sistema de nomes de domínio (DNS) de uma rede de computadores for corrompido por meio de técnica denominada DNS *cache poisoning*, fazendo que esse sistema interprete incorretamente a URL (*uniform resource locator*) de determinado sítio, esse sistema pode estar sendo vítima de *pharming*.

Comentários

O **DNS** (*Domain Name System* – Sistema de Nome de Domínio) é utilizado para traduzir endereços de domínios da Internet, como www.pontodosconcursos.com.br, em endereços IP, como 200.234.196.65. Imagine se tivéssemos que "decorar" todos os IP's dos endereços da Internet que normalmente visitamos!!

O *Pharming* envolve algum tipo de redirecionamento da vítima para *sites* fraudulentos, através de alterações nos serviços de resolução de nomes (DNS). Complementando, é a técnica de infectar o DNS para que ele lhe direcione para um *site* fantasma que é idêntico ao original.

Gabarito: item correto.

72. **(CESPE/2008/PRF/Policial Rodoviário Federal)** Quando enviado na forma de correio eletrônico para uma quantidade considerável de destinatários, um hoax pode ser considerado um tipo de spam, em que o spammer cria e distribui histórias falsas, algumas delas denominadas lendas urbanas.

Comentários

Os ***hoaxes*** **(boatos)** são *e-mails* que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe. Isto ocorre, muitas vezes, porque aqueles que o recebem: confiam no remetente da mensagem; não verificam a procedência da mensagem; não checam a veracidade do conteúdo da mensagem.

Spam é o envio em massa de mensagens de correio eletrônico (*e-mails*) NÃO autorizadas pelo destinatário.

Portanto, o *hoax* pode ser considerado um *spam*, quando for enviado em massa para os destinatários, de forma não-autorizada.

Gabarito: item correto.

73. **(CESPE/2008/TRT-1ªR/Analista Judiciário)** Os arquivos denominados *cookies*, também conhecidos como cavalos de troia, são vírus de computador, com intenção maliciosa, que se instalam no computador sem a autorização do usuário, e enviam, de forma automática e imperceptível, informações do computador invadido.

Comentários

Cookies não são vírus, e sim arquivos lícitos que permitem a identificação do computador cliente no acesso a uma página. Podem ser utilizados para guardar preferências do usuário, bem como informações técnicas como o nome e a versão do *browser* do usuário.

Gabarito: item errado.

74. **(CESPE/2008/TRT-1ªR/Analista Judiciário)** Os programas denominados *worm* são, atualmente, os programas de proteção contra vírus de computador mais eficazes, protegendo o computador contra vírus, cavalos de troia e uma ampla gama de softwares classificados como malware.

Comentários

O antivírus seria a resposta correta nesse item. O *worm* é um tipo específico de *malware*.

Gabarito: item errado.

75. **(CESPE/2004/Polícia Rodoviária Federal)**

Um usuário da Internet, desejando realizar uma pesquisa acerca das condições das rodovias no estado do Rio Grande do Sul, acessou o sítio do Departamento de Polícia Rodoviária Federal — http://www.dprf.gov.br —, por meio do Internet Explorer 6, executado em um computador cujo sistema operacional é o Windows XP e que dispõe do conjunto de aplicativos Office XP. Após algumas operações nesse sítio, o usuário obteve a página Web mostrada na figura acima, que ilustra uma janela do Internet Explorer 6. Considerando essa figura, julgue os itens seguintes, relativos à Internet, ao Windows XP, ao Office XP e a conceitos de segurança e proteção na Internet. I. Sabendo que o mapa mostrado na página Web consiste em uma figura no formato jpg inserida na página por meio de recursos da linguagem HTML, ao se clicar com o botão direito do mouse sobre esse objeto da página, será exibido um menu que disponibiliza ao usuário um menu secundário contendo uma lista de opções que permite exportar de forma automática tal objeto, como figura, para determinados aplicativos do Office XP que estejam em execução concomitantemente ao Internet Explorer 6. A lista de aplicativos do Office XP disponibilizada no menu secundário contém o Word 2002, o Excel 2002, o Paint e o PowerPoint 2002.

Comentários

Ao clicar com o botão direito do mouse é aberto um menu de contexto, mas não é exibida a opção de exportar a figura para qualquer aplicativo do Office. Também aparece outro erro na questão ao afirmar que o Paint faz parte do pacote Office, o que não está correto.

Gabarito: item errado.

76. **(CESPE/2004/Polícia Rodoviária Federal)** II. Para evitar que as informações obtidas em sua pesquisa, ao trafegarem na rede mundial de computadores, do servidor ao cliente, possam ser visualizadas por quem estiver monitorando as operações realizadas na Internet, o usuário tem à disposição diversas ferramentas cuja eficiência varia de implementação para implementação. Atualmente, as ferramentas que apresentam melhor desempenho para a funcionalidade mencionada são as denominadas sniffers e backdoors e os sistemas ditos firewall, sendo que, para garantir tal eficiência, todas essas ferramentas fazem uso de técnicas de criptografia tanto no servidor quanto no cliente da aplicação Internet.

Comentários

Os ***sniffers*** (capturadores de quadros) são dispositivos ou programas de computador que capturam quadros nas comunicações realizadas em uma rede de computadores, armazenando tais quadros para que possam ser analisados posteriormente por quem instalou o *sniffer*. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

O *backdoor* ("porta dos fundos") é um programa que, colocado no micro da vítima, cria uma ou mais falhas de segurança, para permitir que o invasor que o colocou possa facilmente "voltar" àquele computador em um momento seguinte.

Portanto, ao contrário do que o item II afirma, os *sniffers* e *backdoors* não serão utilizados para evitar que informações sejam visualizadas na máquina.

Gabarito: item errado.

77. **(CESPE/2004/Polícia Rodoviária Federal)** III. Por meio da guia Privacidade, acessível quando Opções da Internet é clicada no menu Ferramentas, o usuário tem acesso a recursos de configuração do Internet Explorer 6 que permitem definir procedimento específico que o aplicativo deverá realizar quando uma página Web tentar copiar no computador do usuário arquivos denominados *cookies*. Um *cookie* pode ser definido como um arquivo criado por solicitação de uma página Web para armazenar informações no computador cliente, tais como determinadas preferências do usuário quando ele visita a mencionada página Web. Entre as opções de configuração possíveis, está aquela que impede que os *cookies* sejam armazenados pela página Web. Essa opção, apesar de permitir aumentar, de certa forma, a privacidade do usuário, poderá impedir a correta visualização de determinadas páginas Web que necessitam da utilização de *cookies*.

Comentários

Ao acessar o menu Ferramentas -> Opções da Internet, e, em seguida, clicar na aba (guia) Privacidade, pode-se definir o nível de privacidade do Internet Explorer, possibilitando ou não a abertura de determinadas páginas da Web. O texto correspondente aos cookies está correto.

Gabarito: item correto.

78. **(CESPE/2009-03/TRE-MG)** A instalação de antivírus garante a qualidade da segurança no computador.

Comentários

O antivírus é uma das medidas que podem ser úteis para melhorar a segurança do seu equipamento, desde que esteja atualizado.

Gabarito: item errado.

79. **(CESPE/2009-03/TRE-MG)** Toda intranet consiste em um ambiente totalmente seguro porque esse tipo de rede é restrito ao ambiente interno da empresa que implantou a rede.

Comentários

Não podemos afirmar que a intranet de uma empresa é totalmente segura, depende de como foi implementada.

Gabarito: item errado.

80. **(CESPE/2009-03/TRE-MG)** O upload dos arquivos de atualização é suficiente para a atualização do antivírus pela Internet.

Comentários

O *upload* implica na transferência de arquivo do seu computador para um computador remoto na rede, o que não é o caso da questão.

Gabarito: item errado.

81. **(CESPE/2009-03/TRE-MG)** O *upload* das assinaturas dos vírus detectados elimina-os.

Comentários

Existem dois modos de transferência de arquivo: *upload* e *download*.

O ***upload*** é o termo utilizado para designar a transferência de um dado de um computador local para um equipamento remoto.
O ***download*** é o contrário, termo utilizado para designar a transferência de um dado de um equipamento remoto para o seu computador.
Exemplo: -se queremos enviar uma informação para o servidor de FTP -> estamos realizando um *upload*; -se queremos baixar um arquivo mp3 de um servidor -> estamos fazendo *download*.

Não será feito *upload* de assinaturas de vírus para a máquina do usuário. U**m** programa antivírus é capaz de detectar a presença de *malware* (vírus, vermes, cavalos de troia etc.) em *e-mails* ou arquivos do computador. Esse utilitário conta, muitas vezes, com a vacina capaz de "matar" o *malware* e deixar o arquivo infectado sem a ameaça.

Gabarito: item errado.

82. **(CESPE/2009/TRE-MG)** Os antivírus atuais permitem a atualização de assinaturas de vírus de forma automática, sempre que o computador for conectado à Internet.

Comentários

Alguns fornecedores de programas antivírus distribuem atualizações regulares do seu produto. Muitos programas antivírus têm um recurso de atualização automática. Quando o programa antivírus é atualizado, informações sobre novos vírus são adicionadas a uma lista de vírus a serem verificados. Quando não possui a vacina, ele, pelo menos, tem como detectar o vírus, informando ao usuário acerca do perigo que está iminente.

Gabarito: item correto.

83. **(CESPE/2009/ANATEL/TÉCNICO ADMINISTRATIVO)** Com o desenvolvimento da Internet e a migração de um grande número de sistemas especializados de informação de grandes organizações para sistemas de propósito geral acessíveis universalmente, surgiu a preocupação com a segurança das informações no ambiente da Internet. Acerca da segurança e da tecnologia da informação, julgue o item seguinte.

    A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los.

Comentários

O trecho que define a disponibilidade como "a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário" está correto, no entanto, a afirmativa de que a integridade é "a garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los" é falsa (nesse caso o termo correto seria **confidencialidade**!).

A **disponibilidade** garante que a informação e todos os canais de acesso à ela estejam sempre disponíveis quando um usuário autorizado quiser acessá-la. Como dica para memorização, temos que a confidencialidade é o segredo e a disponibilidade é poder acessar o segredo quando se desejar!!

Já a **integridade** garante que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais, indevidas ou acidentais a informação. Em outras palavras, a informação deve manter todas as características originais durante sua existência. Estas características originais são as estabelecidas pelo proprietário da informação quando da criação ou manutenção da informação (se a informação for alterada por quem possui tal direito, isso não invalida a integridade, ok!!).

Gabarito: item errado.

84. **(CESPE/2009/IBAMA/ANALISTA AMBIENTAL)** Para criar uma cópia de segurança da planilha, também conhecida como backup, é suficiente clicar a ferramenta .

Comentários

Backup refere-se à cópia de dados de um dispositivo para o outro com o objetivo de posteriormente os recuperar (os dados), caso haja algum problema. Essa cópia pode ser realizada em vários tipos de mídias, como CDs, DVSs, fitas DAT etc de forma a protegê-los de qualquer eventualidade. O botão é utilizado para salvar um documento!!

Gabarito: item errado.

85. **(CESPE/2009/MMA)** Antivírus, *worms*, *spywares* e *crackers* são programas que ajudam a identificar e combater ataques a computadores que não estão protegidos por *firewalls*.

Comentários

Os **antivírus** são programas de proteção contra vírus de computador bastante eficazes, protegendo o computador contra vírus, cavalos de troia e uma ampla gama de softwares classificados como malware. Como exemplos cita-se

McAfee Security Center Antivírus, Panda Antivírus, Norton Antivírus, Avira Antivir Personal, AVG etc.

Já os *worms* e *spywares* são programas classificados como *malware*, tendo-se em vista que executam ações mal-intencionadas em um computador!!

- ***Worms***: são programas parecidos com vírus, mas que na verdade são capazes de se propagarem automaticamente através de redes, enviando cópias de si mesmo de computador para computador (observe que os *worms* apenas se copiam, não infectam outros arquivos, eles mesmos são os arquivos!!). Além disso, geralmente utilizam as redes de comunicação para infectar outros computadores (via *e-mails*, Web, FTP, redes das empresas etc).

  Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

- ***Spyware*:** programa que tem por finalidade monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Os ***Crackers*** são indivíduos dotados de sabedoria e habilidade para desenvolver ou alterar sistemas, realizar ataques a sistemas de computador, programar vírus, roubar dados bancários, informações, entre outras ações maliciosas.

Gabarito: item errado.

86. **(CESPE/2009/MMA)** A responsabilidade pela segurança de um ambiente eletrônico é dos usuários. Para impedir a invasão das máquinas por vírus e demais ameaças à segurança, basta que os usuários não divulguem as suas senhas para terceiros.

Comentários

Tanto a empresa que cria e hospeda o ambiente eletrônico, quanto os usuários desse ambiente, devem entender a importância da segurança, atuando como guardiões da rede!!

Gabarito: item errado.

87. **(FCC/TRE-CE/Técnico Judiciário/Programação de Sistemas/2012)** Sobre segurança da informação, analise:

I. É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

II. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída aumenta a eficácia da implementação de um controle de acesso centralizado.

III. Os controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

IV. É importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes.

Está correto o que consta em

a) I, II, III e IV.

b) I, III e IV, apenas

c) I e IV, apenas.

d) III e IV, apenas.

e) I e II, apenas.

Comentários

A única assertiva indevida é a II. A tendência da computação distribuída REDUZ a eficácia da implementação de um controle de acesso centralizado.

Gabarito: letra B.

88. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Em relação à segurança da informação, considere:

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

Comentários

Vamos à caracterização dos princípios destacados na questão:

Item I. **Confidencialidade (sigilo):** é a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las. Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não-autorizadas. Exemplo: o número do seu cartão de crédito só poderá ser conhecido por você e pela loja onde é usado. Se esse número for descoberto por alguém mal-intencionado, o prejuízo causado pela perda de confidencialidade poderá ser elevado, já que poderão se fazer passar por você para realizar compras pela Internet, proporcionando-lhe prejuízos financeiros e uma grande dor de cabeça!

Item II. **Integridade:** esse princípio destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção CONTRA MUDANÇAS INTENCIONAIS, INDEVIDAS OU ACIDENTAIS. Em outras palavras, é a garantia de que a informação que foi armazenada é a que será recuperada!!! O fato de se ter a informação exposta, com alterações não aprovadas e fora do controle do proprietário da informação por pessoa não autorizada está relacionada a esse princípio.

Observe que a quebra de integridade pode ser considerada sob 2 aspectos:

3. alterações nos elementos que suportam a informação - são feitas alterações na estrutura física e lógica em que uma informação está armazenada. Por exemplo quando são alteradas as configurações de um sistema para ter acesso a informações restritas;
4. alterações do conteúdo dos documentos:
   - ex1.: imagine que alguém invada o *notebook* que está sendo utilizado para realizar a sua declaração do Imposto de Renda deste ano, e, momentos antes de você enviá-la para a Receita Federal a mesma é alterada sem o seu consentimento! Neste caso, a informação não será transmitida da maneira adequada, o que quebra o princípio da integridade;
   - ex2: alteração de *sites* por *hackers* (*vide* a figura seguinte, retirada de http://www.g1.globo.com). Acesso em jun. 2011.

Figura. Site da Cia - agência de inteligência do governo Americano - que teve seu conteúdo alterado indevidamente em jun. 2011.

Item III. **Autenticidade:** é a capacidade de garantir a IDENTIDADE de uma pessoa (física ou jurídica) que acessa as informações do sistema ou de um servidor (computador) com quem se estabelece uma transação (de comunicação, como um *e-mail*, ou comercial, como uma venda *on-line*). **É por meio da autenticação que se confirma a identidade da pessoa ou entidade que presta ou acessa as informações.**

Gabarito: letra A.

89. **(FCC/TRT-MS/Analista Sistemas/2006)** Segundo a NBR ISO/IEC 17799:2001, o conceito de segurança da informação é caracterizado pela preservação de:

I.que é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

II.que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

III.que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Preencham correta e respectivamente as lacunas I, II e III:

(a)disponibilidade – integridade – confidencialidade

(b)confidencialidade – integridade – disponibilidade

(c)integridade – confidencialidade – disponibilidade

(d)confidencialidade – disponibilidade - integridade

(e) disponibilidade - confidencialidade – integridade

Comentários

Agora ficou bem fácil!! Mais uma vez, em outras palavras, para memorizar ☺!

Item I. Está relacionando o princípio da **confidencialidade (**ou **sigilo),** que irá prevenir o acesso não autorizado à informação.

Item II. A **integridade** irá prevenir a alteração ou modificação não autorizada (acidental ou não) da informação e de todo o ambiente que suporta a informação. Observe que há várias maneiras de se alterar uma mensagem: modificar uma parte, inserir texto novo, reordenar a mensagem, retransmissão de mensagem antiga etc.

A integridade pode ser comprometida de duas maneiras:

- **alteração maliciosa:** quando um atacante altera a mensagem armazenada ou em trânsito. No caso da alteração maliciosa, a maior preocupação, em geral, é detectar ataques ativos (alteração de dados) muito mais do que corrigir a modificação. Quando um ataque é detectado, deve-se parar o ataque e depois retransmitir a mensagem;
- **alteração acidental:** pode acontecer, por exemplo, por erros de transmissão ou corrupção de dados armazenados. Em relação à alteração acidental, muitos protocolos de transmissão incluem códigos de detecção e/ou correção de erros, isto é, parte da mensagem destina-se a detectar se esta foi alterada (detecção de erro) e, em alguma medida, corrigir os erros.

Item III. Está relacionado à **disponibilidade**, que permite acesso autorizado à informação sempre que necessário!

Gabarito: letra B.

90. **(FCC/TRT-24ª Região/Analista Judiciário/Tecnologia da Informação/2011/Adaptada)** Considere:

I. Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

II. Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

III. Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Na ISO/IEC 17799(renomeada para 27002), I, II e III correspondem, respectivamente, a

a) disponibilidade, integridade e confiabilidade.

b) confiabilidade, integridade e distributividade.

c) confidencialidade, integridade e disponibilidade.

d) confidencialidade, confiabilidade e disponibilidade.

e) integridade, confiabilidade e disponibilidade.

Comentários
Bem, pessoal, se pararam para analisar, essa questão é idêntica à de 2006. Recapitulando temos:

Princípio básico	Conceito	Objetivo
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.	Proteger contra o acesso não autorizado, mesmo para dados em trânsito.
Integridade	Propriedade de salvaguarda da exatidão e completeza de ativos	Proteger informação contra modificação sem permissão; garantir a fidedignidade das informações.
Disponibilidade	Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada	Proteger contra indisponibilidade dos serviços (ou degradação); garantir aos usuários com autorização, o acesso aos dados.

Gabarito: letra C.

91. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Em relação à vulnerabilidades e ataques a sistemas computacionais, é correto afirmar:

a) Medidas de segurança podem ser definidas como ações que visam eliminar riscos para evitar a concretização de uma vulnerabilidade.

b) O vazamento de informação e falha de segurança em um *software* constituem vulnerabilidades.

c) Roubo de informações e perda de negócios constitui ameaças.

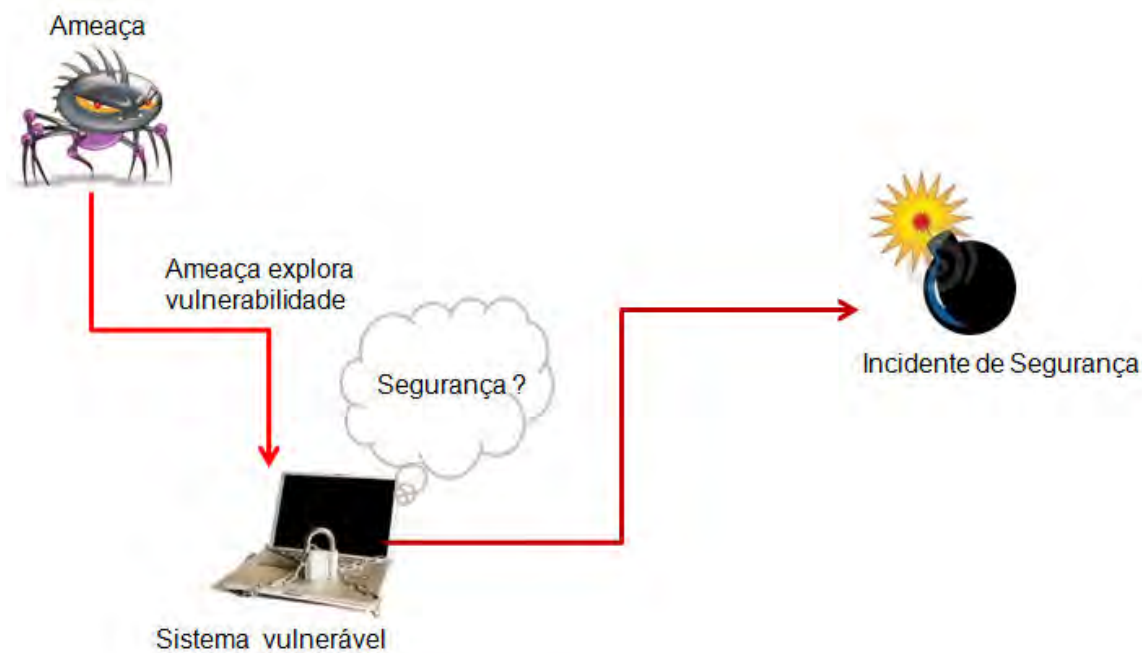
d) Medidas de segurança podem ser definidas como ações que visam eliminar vulnerabilidades para evitar a concretização de uma ameaça.

e) Área de armazenamento sem proteção e travamento automático da estação após período de tempo sem uso constituem ameaça.

Comentários
Item A. Item errado. Os **ATIVOS** são os elementos que sustentam a operação do negócio e estes sempre trarão consigo **VULNERABILIDADES** que, por sua

vez, submetem os ativos a **AMEAÇAS**. **Vulnerabilidade** é uma evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio, aumentando a probabilidade de sucesso pela investida de uma ameaça.

Nesse contexto, medidas de segurança podem ser definidas como ações que visam eliminar vulnerabilidades para evitar a concretização de uma ameaça.

Item B. Item errado. O vazamento de informação é uma ameaça e a falha de segurança em um *software* uma **vulnerabilidade** (**fragilidade** que poderia ser explorada por uma ameaça para concretizar um ataque).

Item C. Item errado. São impactos sobre o negócio da organização.

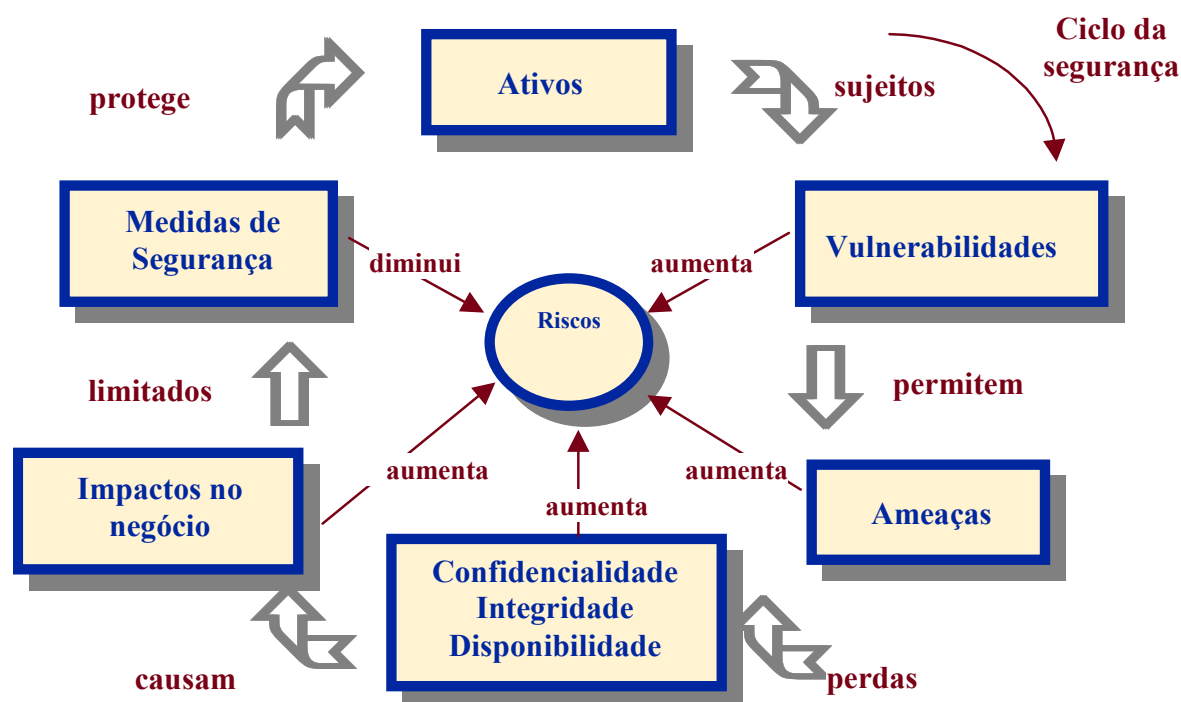



Figura. Ciclo da Segurança da Informação. Fonte: (MOREIRA, 2001)

Item D. Item correto, conforme comentário anterior.

Item E. Item errado. Área de armazenamento sem proteção é uma vulnerabilidade e travamento automático da estação após período de tempo sem uso constitui uma medida de segurança.

Gabarito: letra D.

92. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Ao elaborar e comunicar uma Política de Segurança da Informação - PSI é necessário usar uma linguagem conhecida e meios adequados aos tipos de mensagens e usuários; adotar estilo simples e claro; respeitar o interlocutor sem superestimá-lo nem subestimá-lo; respeitar a cultura organizacional e a do país a que se destina. Nesse sentido, é correto concluir que tal afirmação

a) adere parcialmente às expectativas de uma PSI, pois a política deve ser única, e não deve levar em conta características humanas e legais do país no qual ela é aplicada.

b) adere parcialmente às expectativas de uma PSI, tendo em vista que ela deve ser construída considerando uma linguagem tecnológica desvinculada de adoção de estilos.

c) adere integralmente a formulação de uma PSI, pois ao elaborar uma política é necessário que ela seja ajustada a cada instituição e deve ser comunicada de maneira que todos entendam.

d) adere parcialmente às expectativas de uma PSI, porque os atributos do interlocutor não devem constituir relevância, já que todos os usuários, presumivelmente, foram selecionados pela empresa para entenderem a tecnologia usada.

e) não atende aos propósitos de uma PSI, pois linguagem, estilo e interlocutor não podem sobrepor-se à linguagem tecnológica e é preciso levar em conta a cultura do país no qual ela é aplicada, a linguagem tecnológica utilizada e os níveis de sensibilidade de cada tipo de interlocutor.

Comentários

TCU (2007) destaca que a **Política de Segurança de Informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos**. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações.

A política de segurança da informação tem como objetivo prover uma orientação e apoio da direção para a segurança da informação de acordo com

os requisitos do negócio e com as leis e regulamentações relevantes" (ABNT NBR ISO/IEC 27002:2005).

Gabarito: letra C.

93. **(FCC/2012/TRT-11ª.Região/Provas de Analista Judiciário e Técnico Judiciário)** Quando o cliente de um banco acessa sua conta corrente através da internet, é comum que tenha que digitar a senha em um teclado virtual, cujas teclas mudam de lugar a cada caractere fornecido. Esse procedimento de segurança visa evitar ataques de

(A) spywares e adwares.

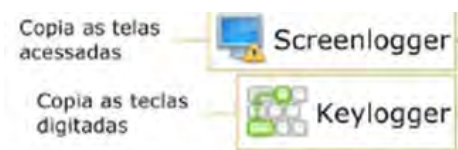
(B) keyloggers e adwares.

(C) screenloggers e adwares.

(D) phishing e pharming.

(E) keyloggers e screenloggers.

Comentários

Já vimos a definição de todas as ameaças nesta aula. O teclado virtual é uma forma de prevenção contra os programas maliciosos (malwares) **keyloggers** (capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador) e **screenloggers** (que tentam coletar dados vindos da tela do computador). Portanto, a letra E é a resposta da questão!

Gabarito: letra E.

94. **(FCC/2011/TRE-TO/Analista Judiciário – Judiciária)** Uma das formas de proteger o sigilo da informação que trafega na Internet é:

a) não fazer os *downloads* em *notebooks*.

b) não responder *e-mails* que chegam "com cópia oculta".

c) mandar *e-mails* somente a pessoas da lista pessoal.

d) não usar a opção "com cópia para" do correio eletrônico.

e) a criptografia

Comentários

Ao enviar informações sigilosas via internet deve-se utilizar de um sistema que faça a codificação (chave, cifra), de modo que somente as máquinas que conhecem o código consigam decifrá-lo. É a criptografia, portanto, a medida de

segurança a ser adotada para resguardar o sigilo da informação que trafega pela Internet.

Gabarito: letra E.

95. **(FCC/2011/TRF - 1.ª Região/Técnico Judiciário – Segurança e Transporte)** Considerando o recebimento de um arquivo executável de fonte desconhecida, no correio eletrônico, a atitude mais adequada diante deste fato é

a) não executá-lo;

b) baixá-lo no seu desktop e executá-lo localmente, somente;

c) repassá-lo para sua lista de endereços solicitando aos mais experientes que o executem;

d) executá-lo diretamente, sem baixá-lo no seu desktop;

e) executá-lo de qualquer forma, porém comunicar o fato ao administrador de sua rede.

Comentários

O arquivo executável, que está sendo recebido de uma fonte desconhecida, no correio eletrônico, pode conter um código malicioso (como um vírus ou um cavalo de troia, etc.), que, ao ser executado, tem grande probabilidade de causar algum problema que resulte na violação da segurança do computador. Desconfie sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo em anexo pode ser malicioso. Portanto nunca abra arquivos ou execute programas anexados aos e-mails, sem antes verificá-los com um bom programa antivírus (atualizado!). Diante disso, a resposta certa é a letra A.

Gabarito: letra A.

96. **(FCC/2009/MPSED/Analista do Ministério Público/Analista de Sistemas)** Consiste em um conjunto de computadores interconectados por meio de uma rede relativamente insegura que utiliza a criptografia e protocolos especiais para fornecer segurança. Esta é uma conceituação básica para:

a) rede privada com comunicação criptográfica simétrica;

b) canal privado de comunicação assimétrica;

c) canal privado de comunicação síncrona;

d) rede privada com autenticação digital;

e) rede privada virtual.

Comentários
Uma **VPN** (***Virtual Private Network* – Rede Privada Virtual**) é uma rede **privada** (não é de acesso público!) que usa a infraestrutura de uma rede pública já existente (como, por exemplo, a **Internet**) para transferir seus dados (os dados devem estar **criptografados** para passarem despercebidos e inacessíveis pela Internet).

As VPNs são muito utilizadas para interligar filiais de uma mesma empresa, ou fornecedores com seus clientes (em negócios eletrônicos), por meio da estrutura física de uma rede pública.

O tráfego de dados é levado pela rede pública utilizando protocolos não necessariamente seguros. VPNs seguras usam protocolos de criptografia por tunelamento, que *fornecem confidencialidade (sigilo), autenticação e integridade* necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, esses protocolos podem assegurar comunicações seguras por meio de redes inseguras.

Gabarito: letra E.

97. **(Elaboração própria)** Trata-se de um software malicioso que, ao infectar um computador, criptografa todo ou parte do conteúdo do disco rígido. Os responsáveis por esse software exigem da vítima um pagamento pelo "resgate" dos dados.

a) bot;

b) DoS;

c) DDoS;

d) pharming;

e) ransomware.

Comentários
Item A. ***Bot***: robô. É um *worm* que dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente. Os *bots* esperam por comandos de um *hacker*, podendo manipular os sistemas infectados, sem o conhecimento do usuário. Nesse ponto, cabe destacar um termo que já foi cobrado várias vezes em prova!! Trata-se do significado do termo ***botnet***, junção da contração das palavras *robot* (*bot*) e *network* (*net*). Uma rede infectada por *bots* é denominada de *botnet* (também conhecida como rede *zumbi*), sendo composta geralmente por milhares desses elementos maliciosos que ficam residentes nas máquinas, aguardando o comando de um invasor. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço, etc. Item **ERRADO**.

Item B. **DoS** (*Denial of Service* – Negação de Serviço): é a forma mais conhecida de *ataque*, que consiste na perturbação de um serviço. O atacante utiliza *um computador*, a partir do qual ele envia vários pacotes ou requisições de serviço de uma vez, para tirar de operação um serviço ou computador (es) conectado(s) à Internet, causando prejuízos. Para provocar um DoS, os atacantes disseminam vírus, gerando grandes volumes de tráfego de forma artificial, ou muitos pedidos aos servidores, que causam sobrecarga e estes últimos ficam impedidos de processar os pedidos normais. Item **ERRADO**.

Item C. **DDoS** (*Distributed Denial of Service* – Negação de Serviço Distribuído): é um ataque DoS ampliado, ou seja, que utiliza até milhares de computadores para tirar de operação um ou mais serviços ou computadores conectados à Internet. Normalmente, procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede. Item **ERRADO**.

Item D. ***Pharming* (DNS *Cache Poisoning* – Envenenamento de *Cache* DNS)**: é um ataque que consiste basicamente em modificar a relação entre o nome de um site ou computador e seu endereço IP correspondente. Neste ataque, um servidor de nomes (*servidor DNS*) é *comprometido*, de tal forma que as requisições de acesso a um site feitas pelos usuários desse servidor sejam redirecionadas a outro endereço. Um ataque *pharming* também pode alterar o arquivo *hosts* – localizado no computador do usuário –, manipulando os endereços IPs correspondentes às suas devidas URLs.

Ex.: Ao atacar um servidor DNS, o IP do site www.teste.com.br poderia ser mudado de 65.150.162.57 para 209.86.194.103, enviando o usuário para a página relacionada ao IP incorreto. Item **ERRADO**.

Item E. ***Ransomwares*** são ferramentas para crimes de extorsão extremamente ilegais. O *ransomware* funciona da seguinte forma:

- ele procura por diversos tipos de arquivos no HD (disco rígido) do computador atacado e os *comprime em um arquivo protegido por senha*;
- a partir daí, a vítima é pressionada a depositar quantias em contas do tipo *e-gold* (contas virtuais que utilizam uma unidade monetária específica e que podem ser abertas por qualquer um na rede sem grandes complicações);
- uma vez pagos, os criminosos fornecem a senha necessária para que os dados voltem a ser acessados pela vítima.

Item **CERTO**. Eis a resposta da questão!

Gabarito: letra E.

98. **(FCC/2008/TCE-SP/Adaptada)** Em relação a Certificado Digital, é correto afirmar que: [os certificados servem para garantir a segurança dos dados enviados via upload].

Comentários

A afirmativa está **ERRADA**. Quanto aos objetivos do certificado digital, podemos destacar:

- vincular uma chave pública a um titular (esse é o objetivo principal!);
- transferir credibilidade, que hoje é baseada em papel e conhecimento, para o ambiente eletrônico;
- assinar digitalmente um documento eletrônico, atribuindo validade jurídica a ele.

Gabarito: item errado.

99. **(FCC/2008/TCE-SP/Adaptada)** Em relação a Certificado Digital, é correto afirmar que: são *plugins* que definem a qualidade criptográfica das informações que trafegam na WWW.

Comentários

A afirmativa está errada. O ***plug-in*** é um software que adiciona recursos computacionais a um cliente ou *browser* da WWW. A maioria dos *plug-ins* está disponível gratuitamente na própria Internet. É necessário, por exemplo, que o usuário instale um *plug-in* para poder visualizar videoclipes em MPG (ou MPEG).

Gabarito: item errado.

100. **(FCC/2008/TCE-SP)** *Secure Sockets Layer* trata-se de

a) qualquer tecnologia utilizada para proteger os interesses de proprietários de conteúdo e serviços;

b) um elemento de segurança que controla todas as comunicações que passam de uma rede para outra e, em função do que sejam, permite ou denega a continuidade da transmissão;

c) uma técnica usada para garantir que alguém, ao realizar uma ação em um computador, não possa falsamente negar que realizou aquela ação;

d) uma técnica usada para examinar se a comunicação está entrando ou saindo e, dependendo da sua direção, permiti-la ou não;

e) um protocolo que fornece comunicação segura de dados através de criptografia do dado.

Comentários

O **SSL** (*Secure Sockets Layer – Camada de conexões seguras*) é um protocolo de criptografia que pode ser utilizado para prover segurança na comunicação de qualquer aplicação baseada em TCP. O SSL está posicionado entre a camada de transporte e a camada de aplicação da pilha TCP/IP e funciona provendo serviços de autenticação do servidor, comunicação secreta e integridade dos dados.

Cabe destacar que o **HTTPS** (HTTP Seguro) é usado para realizar o acesso a sites (como de bancos on-line e de compras) com transferência criptografada de dados. O HTTPS nada mais é do que a junção dos protocolos HTTP e SSL (HTTP over SSL). O HTTPS geralmente utiliza a porta TCP 443, em vez da porta 80 utilizada pelo protocolo HTTP. A resposta à questão é, como já visto, a letra E!

Gabarito: letra E.

CONSIDERAÇÕES FINAIS

Por hoje ficamos por aqui.

Espero que esse material, feito com todo o carinho, ajude-o a entender melhor o funcionamento das ameaças virtuais e principais medidas de segurança que devem ser adotadas para se proteger dessas ameaças, e o ajude a acertar as questões de segurança da sua prova!

Um grande abraço,

Prof[a] Patrícia Lima Quintão

BIBLIOGRAFIA

QUINTÃO, PATRÍCIA LIMA. **Notas de aula**, 2012/2013.

QUINTÃO, PATRÍCIA LIMA. **Informática-FCC-Questões Comentadas e Organizadas por Assunto**, 2ª. Edição. Ed. Gen/Método, 2012.

CERTBR. Disponível em: <http://**cartilha**.cert.br/ >.2006. Acesso em: out. 2012.

CHESWICK, W. R., BELLOVIN, S. M. e RUBIN, A. D. **Firewalls e Segurança na Internet: repelindo o hacker ardiloso**. Ed. Bookman, 2ª Ed., 2005.

GUIMARÃES, A. G., LINS, R. D. e OLIVEIRA, R. **Segurança com Redes Privadas Virtuais (VPNs)**. Ed. Brasport, Rio de Janeiro, 2006.

IMONIANA, J. o. **Auditoria de Sistemas de Informações**.

Infowester. Disponível em: http://www.infowester.com.br.

INFOGUERRA. **Vírus de celular chega por mensagem multimídia**. 2005. Disponível em: http://informatica.terra.com.br/interna/0,,OI484399-EI559,00.html. Acesso em: dez. 2011.

LISTA DE QUESTÕES APRESENTADAS NA AULA

1. **(CESPE/2013/TRT-10RJ/Analista)** A transferência de arquivos para pendrives constitui uma forma segura de se realizar becape, uma vez que esses equipamentos não são suscetíveis a malwares.

2. **(CESPE/2013/TRT-10RJ/Analista)** As características básicas da segurança da informação — confidencialidade, integridade e disponibilidade — não são atributos exclusivos dos sistemas computacionais.

3. **(CESPE/2013/TRT-10RJ/Analista)** O vírus de computador é assim denominado em virtude de diversas analogias poderem ser feitas entre esse tipo de vírus e os vírus orgânicos.

4. **(CESPE/2013/TRT-10RJ/Analista)** Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

5. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Para garantir que os computadores de uma rede local não sofram ataques vindos da Internet, é necessária a instalação de firewalls em todos os computadores dessa rede.

6. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Ao se realizar um procedimento de backup de um conjunto de arquivos e pastas selecionados, é possível que o conjunto de arquivos e pastas gerado por esse procedimento ocupe menos espaço de memória que aquele ocupado pelo conjunto de arquivos e pastas de que se fez o backup.

7. **(Cespe/Câmara dos Deputados/ Arquiteto e Engenheiros/2012)** Os worms, assim como os vírus, infectam computadores, mas, diferentemente dos vírus, eles não precisam de um programa hospedeiro para se propagar.

8. **(CESPE/Técnico Administrativo – Nível Médio – PREVIC/2011)** Entre os atributos de segurança da informação, incluem-se a confidencialidade, a integridade, a disponibilidade e a autenticidade. A integridade consiste na propriedade que limita o acesso à informação somente às pessoas ou entidades autorizadas pelo proprietário da informação.

9. **(CESPE/MPE-PI/Técnico Ministerial/Área: Administrativa/ 2012)** Worms são programas maliciosos que se autorreplicam em redes de computadores anexados a algum outro programa existente e instalado em computadores da rede.

10. **(CESPE/2002/POLÍCIA FEDERAL/PERITO: ÁREA 3 . COMPUTAÇÃO)** Sistemas criptográficos são ditos simétricos ou de chave secreta quando a chave utilizada para cifrar é a mesma utilizada para decifrar. Sistemas assimétricos ou de chave pública utilizam chaves distintas para cifrar e decifrar. Algoritmos simétricos são geralmente mais eficientes computacionalmente que os assimétricos e por isso são preferidos para cifrar grandes massas de dados ou para operações online.

11. **(CESPE/Agente Técnico de Inteligência – Área de Tecnologia da Informação – ABIN/2010)** A chave assimétrica é composta por duas chaves criptográficas: uma privada e outra pública.

12. **(CESPE/Oficial Técnico de Inteligência-Área de Arquivologia - ABIN/2010)** A respeito de mecanismos de segurança da informação, e considerando que uma mensagem tenha sido criptografada com a chave pública de determinado destino e enviada por meio de um canal de comunicação, pode-se afirmar que a mensagem criptografada com a chave pública do destinatário garante que somente quem gerou a informação criptografada e o destinatário sejam capazes de abri-la.

13. **(CESPE/2010/Caixa/Técnico Bancário)** O destinatário de uma **mensagem** **assinada** utiliza a chave pública do remetente para garantir que essa mensagem tenha sido enviada pelo próprio remetente.

14. **(CESPE/2010/Caixa/Técnico Bancário)** A assinatura digital facilita a identificação de uma comunicação, pois baseia-se em criptografia simétrica de uma única chave.

15. **(CESPE/TCU/Técnico Federal de Controle Externo/2012)** Por meio de certificados digitais, é possível assinar digitalmente documentos a fim de garantir o sigilo das informações contidas em tais documentos.

16. **(CESPE/AL-ES/Procurador/2011)** Caso o usuário acesse uma página na Internet e lhe seja apresentado um certificado digital válido, é correto inferir que a conexão utilizada por esse usuário estará cifrada com o uso de *pendrive.*

17. **(CESPE/Oficial Técnico de Inteligência/Área de Desenvolvimento e Manutenção de Sistemas – ABIN/2010)** As assinaturas digitais atuam sob o princípio básico da confidencialidade da informação, uma vez que conferem a autenticação da identidade do remetente de uma mensagem. No entanto, tal solução não garante a integridade da informação, que deve ser conferida por meio de tecnologias adicionais de criptografia.

18. **(CESPE/Técnico Bancário/Carreira administrativa- Caixa Econômica Federal-NM1/2010)** Para assinar uma mensagem digital, o remetente usa uma chave privada.

19. **(CESPE/AL-ES/Cargos de Nível Médio/2011)** Existem diversos dispositivos que protegem tanto o acesso a um computador quanto a toda uma rede. Caso um usuário pretenda impedir que o tráfego com origem na Internet faça conexão com seu computador pessoal, a tecnologia adequada a ser utilizada nessa situação será o IpV6.

20. **(CESPE/Técnico Administrativo – Nível Médio – PREVIC/2011)** Firewall é o elemento de defesa mais externo na intranet de uma empresa e sua principal função é impedir que usuários da intranet acessem qualquer rede externa ligada à Web.

21. **(CESPE/CBM-DF/Oficial Bombeiro Militar Complementar/Informática/2011)** Em uma VPN (*virtual private network*) que utilize a técnica de tunelamento, os conteúdos dos pacotes que trafegam pela Internet são criptografados, ao passo que, para permitir o roteamento eficiente dos pacotes, os seus endereços de origem e de destino permanecem não criptografados.

22. **(CESPE/MPE-PI/2012)** A adoção de crachás para identificar as pessoas e controlar seus acessos às dependências de uma empresa é um mecanismo adequado para preservar a segurança da informação da empresa.[

23. **(CESPE/Nível Superior - PREVIC/2011)** Por meio do uso de certificados digitais, é possível garantir a integridade dos dados que transitam pela Internet, pois esses certificados são uma forma confiável de se conhecer a origem dos dados.

24. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** Tecnologias como a biometria por meio do reconhecimento de digitais de dedos das mãos ou o

reconhecimento da íris ocular são exemplos de aplicações que permitem exclusivamente garantir a integridade de informações.

25. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** Um filtro de phishing é uma ferramenta que permite criptografar uma mensagem de email cujo teor, supostamente, só poderá ser lido pelo destinatário dessa mensagem.

26. **(CESPE/TJ-ES/CBNS1_01/Superior/2011)** O conceito de confidencialidade refere-se a disponibilizar informações em ambientes digitais apenas a pessoas para as quais elas foram destinadas, garantindo-se, assim, o sigilo da comunicação ou a exclusividade de sua divulgação apenas aos usuários autorizados.

27. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** É necessário sempre que o software de antivírus instalado no computador esteja atualizado e ativo, de forma a se evitar que, ao se instalar um cookie no computador do usuário, essa máquina fique, automaticamente, acessível a um usuário intruso (hacker), que poderá invadi-la.

28. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** Os pop-ups são vírus que podem ser eliminados pelo chamado bloqueador de pop-ups, se este estiver instalado na máquina. O bloqueador busca impedir, por exemplo, que esse tipo de vírus entre na máquina do usuário no momento em que ele consultar um sítio da Internet.

29. **(CESPE/Técnico Administrativo - MPU/2010)** De acordo com o princípio da disponibilidade, a informação só pode estar disponível para os usuários aos quais ela é destinada, ou seja, não pode haver acesso ou alteração dos dados por parte de outros usuários que não sejam os destinatários da informação.

30. **(CESPE/TJ-ES/CBNM1_01/Nível Médio/2011)** Confidencialidade, disponibilidade e integridade da informação, que são conceitos importantes de segurança da informação em ambiente digital, devem estar presentes na gestão e no uso de sistemas de informação, em benefício dos cidadãos e dos fornecedores de soluções.

31. **(CESPE/Nível Superior - STM/2011)** Um firewall pessoal instalado no computador do usuário impede que sua máquina seja infectada por qualquer tipo de vírus de computador.

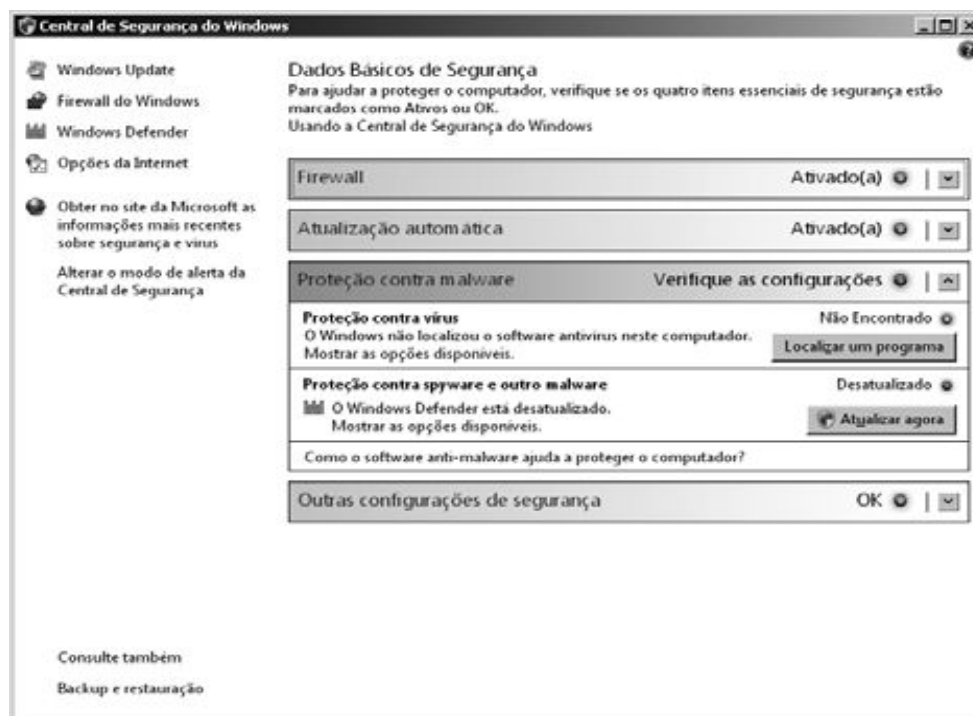
32. **(CESPE/Analista Judiciário - Tecnologia da Informação-TRE-MT/2010)** A confidencialidade tem a ver com salvaguardar a exatidão e a inteireza das informações e métodos de processamento. Para tanto, é necessário que os processos de gestão de riscos identifiquem, controlem, minimizem ou eliminem os riscos de segurança que podem afetar sistemas de informações, a um custo aceitável.

33. **(CESPE/ANALISTA- TRE.BA/2010)** Confidencialidade, disponibilidade e integridade da informação são princípios básicos que orientam a definição de políticas de uso dos ambientes computacionais. Esses princípios são aplicados exclusivamente às tecnologias de informação, pois não podem ser seguidos por seres humanos.

34. **(CESPE/Analista de Saneamento/Analista de Tecnologia da Informação – Desenvolvimento - EMBASA/2010)** O princípio da autenticação em segurança diz que um usuário ou processo deve ser corretamente identificado. Além disso, todo processo ou usuário autêntico está automaticamente autorizado para uso dos sistemas.

35. **(CESPE/Técnico Administrativo - ANATEL/2009)** Com o desenvolvimento da Internet e a migração de um grande número de sistemas especializados de informação de grandes organizações para sistemas de propósito geral acessíveis universalmente, surgiu a preocupação com a segurança das informações no ambiente da Internet. Acerca da segurança e da tecnologia da informação, julgue o item a seguir.

    -> A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los.

(CESPE/Escrivão de Polícia Federal/2010)

Considerando a figura acima, que apresenta uma janela com algumas informações da central de segurança do Windows de um sistema computacional (host) de uso pessoal ou corporativo, julgue os três próximos itens, a respeito de segurança da informação.

36. **(CESPE/2010/Escrivão de Polícia Federal)** A atualização automática disponibilizada na janela exibida acima é uma função que está mais relacionada à distribuição de novas funções de segurança para o sistema operacional do que à distribuição de novos patches (remendos) que corrijam as vulnerabilidades de código presentes no sistema operacional.

37. **(CESPE/2010/Escrivão de Polícia Federal)** Na figura anterior, o firewall assinalado como ativado, em sua configuração padrão, possui um conjunto maior de regras para bloqueio de conexões originadas de fora do computador do que para as conexões originadas de dentro do computador.

38. **(CESPE/2010/Escrivão de Polícia Federal)** A configuração da proteção contra malwares exposta na figura indica que existe no host uma base de assinaturas de vírus instalada na máquina.

39. (CESPE/2010/Caixa/Técnico Bancário/Administrativo) Uma autoridade de registro emite o par de chaves do usuário que podem ser utilizadas tanto para criptografia como para assinatura de mensagens eletrônicas.

40. **(CESPE/Técnico Judiciário/Programação de Sistemas - TRE-MT/2010)** Disponibilidade é a garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas.

41. **(CESPE/TRE-MT/Técnico Judiciário - Programação de Sistemas/2010)** Confidencialidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

42. **(CESPE/UERN/Agente Técnico Administrativo/2010)** A disponibilidade da informação é a garantia de que a informação não será alterada durante o trânsito entre o emissor e o receptor, além da garantia de que ela estará disponível para uso nesse trânsito.

43. **(CESPE/AGU/Contador/2010)** Um arquivo criptografado fica protegido contra contaminação por vírus.

44. **(CESPE/UERN/Agente Técnico Administrativo/2010)** Cavalo de troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.

45. **(CESPE/UERN/Agente Técnico Administrativo/2010)** O uso de um programa anti-spam garante que software invasor ou usuário mal-intencionado não acesse uma máquina conectada a uma rede.

46. **(CESPE/SEDU-ES/Agente de Suporte Educacional/2010)** Vírus é um programa que pode se reproduzir anexando seu código a um outro programa, da mesma forma que os vírus biológicos se reproduzem.

47. **(CESPE/SEDU-ES/Agente de Suporte Educacional/2010)** Cavalos-de-troia, adwares e vermes são exemplos de pragas virtuais.

48. **(CESPE/SEDU-ES/AGENTE DE SUPORTE EDUCACIONAL/2010)** Backup é o termo utilizado para definir uma cópia duplicada de um arquivo, um disco, ou um dado, feita com o objetivo de evitar a perda definitiva de arquivos importantes.

49. **(CESPE/EMBASA/Analista de Saneamento - Analista de TI – Área: Desenvolvimento/2010)** O princípio da autenticação em segurança diz

que um usuário ou processo deve ser corretamente identificado. Além disso, todo processo ou usuário autêntico está automaticamente autorizado para uso dos sistemas.

50. **(CESPE/TRE-MT/Analista Judiciário - Tecnologia da Informação/2010)** Uma das vantagens da criptografia simétrica em relação à assimétrica é a maior velocidade de cifragem ou decifragem das mensagens. Embora os algoritmos de chave assimétrica sejam mais rápidos que os de chave simétrica, uma das desvantagens desse tipo de criptografia é a exigência de uma chave secreta compartilhada.

51. (CESPE/TRE-MT/Analista Judiciário/Tecnologia da Informação/2010) Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é privada e divulgada para o transmissor, enquanto a chave usada para decriptar a mensagem é pública.

52. **(CESPE/CAIXA-NM1/ Técnico Bancário/Carreira administrativa/2010)** Autoridade certificadora é a denominação de usuário que tem poderes de acesso às informações contidas em uma mensagem assinada, privada e certificada.

53. **(CESPE/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA/2010)** A autoridade reguladora tem a função de emitir certificados digitais, funcionando como um cartório da Internet.

54. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** O ITI (Instituto Nacional de Tecnologia da Informação) é também conhecido como Autoridade Certificadora Raiz Brasileira.

55. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** PKI ou ICP é o nome dado ao certificado que foi emitido por uma autoridade certificadora.

56. **(CESPE/2010/CAIXA-NM1/ TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA)** Um certificado digital é pessoal, intransferível e não possui data de validade.

57. **(CESPE/2010/UERN/TÉCNICO DE NÍVEL SUPERIOR-Adaptada)** Vírus, worms e cavalos-de-troia são exemplos de software mal-intencionados que têm o objetivo de, deliberadamente, prejudicar o funcionamento do computador. O firewall é um tipo de malware que ajuda a proteger o computador contra cavalos-de-troia.

58. **(CESPE/2010/UERN/Agente Técnico Administrativo)** Uma das formas de se garantir a segurança das informações de um website é não colocá-lo em rede, o que elimina a possibilidade de acesso por pessoas intrusas.

59. **(CESPE/2010/TRE-MT/Analista Judiciário - Tecnologia da Informação)** A segurança física objetiva impedir acesso não autorizado, danos ou interferência às instalações físicas e às informações da organização. A proteção fornecida deve ser compatível com os riscos identificados, assegurando a preservação da confidencialidade da informação.

60. **(CESPE/2010/TRE-MT/Analista Judiciário - Tecnologia da Informação)** Serviços de não repudiação são técnicas utilizadas para detectar alterações não autorizadas ou corrompimento dos conteúdos de uma mensagem transmitida eletronicamente. Essas técnicas, que têm como base o uso de criptografia e assinatura digital, podem ajudar a estabelecer provas para substanciar se determinado evento ou ação ocorreu.

61. **(CESPE/2010/EMBASA/ANALISTA DE SANEAMENTO)** Um firewall em uma rede é considerado uma defesa de perímetro e consegue coibir todo tipo de invasão em redes de computadores.

62. **(CESPE/2009/TRE/PR/Técnico Judiciário – Especialidade: Operação de computadores)** Firewalls são equipamentos típicos do perímetro de segurança de uma rede, sendo responsáveis pela detecção e contenção de ataques e intrusões.

63. **(CESPE/2008/TRT-1ªR/Analista Judiciário-Adaptada)** Uma característica das redes do tipo VPN (*virtual private networks*) é que elas nunca devem usar criptografia, devido a requisitos de segurança e confidencialidade.

64. **(CESPE/2010/MINISTÉRIO DA SAÚDE /ANALISTA TÉCNICO-ADMINISTRATIVO)** Firewall é o mecanismo usado em redes de

computadores para controlar e autorizar o tráfego de informações, por meio do uso de filtros que são configurados de acordo com as políticas de segurança estabelecidas.

65. **(CESPE/2010/TRE.BA/ANALISTA/Q.27)** Firewall é um recurso utilizado para a segurança tanto de estações de trabalho como de servidores ou de toda uma rede de comunicação de dados. Esse recurso possibilita o bloqueio de acessos indevidos a partir de regras preestabelecidas.

66. **(CESPE/2010/UERN/TÉCNICO DE NÍVEL SUPERIOR-Adaptada)** Firewall é um sistema constituído de software e hardware que verifica informações oriundas da Internet ou de uma rede de computadores e que permite ou bloqueia a entrada dessas informações, estabelecendo, dessa forma, um meio de proteger o computador de acesso indevido ou indesejado.

67. **(CESPE/2010/TRE-BA/Técnico Judiciário - Área Administrativa)** Uma das formas de bloquear o acesso a locais não autorizados e restringir acessos a uma rede de computadores é por meio da instalação de firewall, o qual pode ser instalado na rede como um todo, ou apenas em servidores ou nas estações de trabalho.

68. **(CESPE/2004/POLÍCIA FEDERAL/REGIONAL/PERITO/ÁREA 3/Q. 105)** Um dos mais conhecidos ataques a um computador conectado a uma rede é o de negação de serviço (DoS – *denial of service*), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.

69. **(CESPE/2008/PRF/Policial Rodoviário Federal)** O uso de firewall e de software antivírus é a única forma eficiente atualmente de se implementar os denominados filtros anti-spam.

70. **(CESPE/2008/PRF-POLICIAL RODOVIÁRIO FEDERAL-ADAPTADA)** *Phishing* e *pharming* são pragas virtuais variantes dos denominados cavalos-de-tróia, se diferenciando destes por precisarem de arquivos específicos para se replicar e contaminar um computador e se diferenciando, entre eles, pelo fato de que um atua em mensagens de e-mail trocadas por serviços de webmail e o outro, não.

71. **(CESPE/2008/PRF/Policial Rodoviário Federal)** Se o sistema de nomes de domínio (DNS) de uma rede de computadores for corrompido por meio de técnica denominada DNS *cache poisoning*, fazendo que esse

sistema interprete incorretamente a URL (*uniform resource locator*) de determinado sítio, esse sistema pode estar sendo vítima de *pharming*.

72. **(CESPE/2008/PRF/Policial Rodoviário Federal)** Quando enviado na forma de correio eletrônico para uma quantidade considerável de destinatários, um hoax pode ser considerado um tipo de spam, em que o spammer cria e distribui histórias falsas, algumas delas denominadas lendas urbanas.

73. **(CESPE/2008/TRT-1ªR/Analista Judiciário)** Os arquivos denominados *cookies*, também conhecidos como cavalos de troia, são vírus de computador, com intenção maliciosa, que se instalam no computador sem a autorização do usuário, e enviam, de forma automática e imperceptível, informações do computador invadido.

74. **(CESPE/2008/TRT-1ªR/Analista Judiciário)** Os programas denominados *worm* são, atualmente, os programas de proteção contra vírus de computador mais eficazes, protegendo o computador contra vírus, cavalos de troia e uma ampla gama de softwares classificados como malware.

75. **(CESPE/2004/Polícia Rodoviária Federal)**

Um usuário da Internet, desejando realizar uma pesquisa acerca das condições das rodovias no estado do Rio Grande do Sul, acessou o sítio do Departamento de Polícia Rodoviária Federal — http://www.dprf.gov.br —, por meio do Internet Explorer 6, executado em um computador cujo sistema operacional é o Windows XP e que dispõe do conjunto de aplicativos Office XP. Após algumas operações nesse sítio, o usuário obteve a página Web mostrada na figura acima, que ilustra uma janela do Internet Explorer 6. Considerando essa figura, julgue os itens seguintes, relativos à Internet, ao Windows XP, ao Office

XP e a conceitos de segurança e proteção na Internet. I. Sabendo que o mapa mostrado na página Web consiste em uma figura no formato jpg inserida na página por meio de recursos da linguagem HTML, ao se clicar com o botão direito do mouse sobre esse objeto da página, será exibido um menu que disponibiliza ao usuário um menu secundário contendo uma lista de opções que permite exportar de forma automática tal objeto, como figura, para determinados aplicativos do Office XP que estejam em execução concomitantemente ao Internet Explorer 6. A lista de aplicativos do Office XP disponibilizada no menu secundário contém o Word 2002, o Excel 2002, o Paint e o PowerPoint 2002.

76. **(CESPE/2004/Polícia Rodoviária Federal)** II. Para evitar que as informações obtidas em sua pesquisa, ao trafegarem na rede mundial de computadores, do servidor ao cliente, possam ser visualizadas por quem estiver monitorando as operações realizadas na Internet, o usuário tem à disposição diversas ferramentas cuja eficiência varia de implementação para implementação. Atualmente, as ferramentas que apresentam melhor desempenho para a funcionalidade mencionada são as denominadas sniffers e backdoors e os sistemas ditos firewall, sendo que, para garantir tal eficiência, todas essas ferramentas fazem uso de técnicas de criptografia tanto no servidor quanto no cliente da aplicação Internet.

77. **(CESPE/2004/Polícia Rodoviária Federal)** III. Por meio da guia Privacidade, acessível quando Opções da Internet é clicada no menu Ferramentas, o usuário tem acesso a recursos de configuração do Internet Explorer 6 que permitem definir procedimento específico que o aplicativo deverá realizar quando uma página Web tentar copiar no computador do usuário arquivos denominados *cookies*. Um *cookie* pode ser definido como um arquivo criado por solicitação de uma página Web para armazenar informações no computador cliente, tais como determinadas preferências do usuário quando ele visita a mencionada página Web. Entre as opções de configuração possíveis, está aquela que impede que os *cookies* sejam armazenados pela página Web. Essa opção, apesar de permitir aumentar, de certa forma, a privacidade do usuário, poderá impedir a correta visualização de determinadas páginas Web que necessitam da utilização de *cookies*.

78. **(CESPE/2009-03/TRE-MG)** A instalação de antivírus garante a qualidade da segurança no computador.

79. **(CESPE/2009-03/TRE-MG)** Toda intranet consiste em um ambiente totalmente seguro porque esse tipo de rede é restrito ao ambiente interno da empresa que implantou a rede.

80. **(CESPE/2009-03/TRE-MG)** O upload dos arquivos de atualização é suficiente para a atualização do antivírus pela Internet.

81. **(CESPE/2009-03/TRE-MG)** O *upload* das assinaturas dos vírus detectados elimina-os.

82. **(CESPE/2009/TRE-MG)** Os antivírus atuais permitem a atualização de assinaturas de vírus de forma automática, sempre que o computador for conectado à Internet.

83. **(CESPE/2009/ANATEL/TÉCNICO ADMINISTRATIVO)** Com o desenvolvimento da Internet e a migração de um grande número de sistemas especializados de informação de grandes organizações para sistemas de propósito geral acessíveis universalmente, surgiu a preocupação com a segurança das informações no ambiente da Internet. Acerca da segurança e da tecnologia da informação, julgue o item seguinte.

    A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los.

84. **(CESPE/2009/IBAMA/ANALISTA AMBIENTAL)** Para criar uma cópia de segurança da planilha, também conhecida como backup, é suficiente clicar a ferramenta .

85. **(CESPE/2009/MMA)** Antivírus, *worms*, *spywares* e *crackers* são programas que ajudam a identificar e combater ataques a computadores que não estão protegidos por *firewalls*.

86. **(CESPE/2009/MMA)** A responsabilidade pela segurança de um ambiente eletrônico é dos usuários. Para impedir a invasão das máquinas por vírus e demais ameaças à segurança, basta que os usuários não divulguem as suas senhas para terceiros.

87. **(FCC/TRE-CE/Técnico Judiciário/Programação de Sistemas/2012)** Sobre segurança da informação, analise:

I. É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

II. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída aumenta a eficácia da implementação de um controle de acesso centralizado.

III. Os controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

IV. É importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-business*), e evitar ou reduzir os riscos relevantes.

Está correto o que consta em

a) I, II, III e IV.

b) I, III e IV, apenas

c) I e IV, apenas.

d) III e IV, apenas.

e) I e II, apenas.

88. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Em relação à segurança da informação, considere:

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

89. **(FCC/TRT-MS/Analista Sistemas/2006)** Segundo a NBR ISO/IEC 17799:2001, o conceito de segurança da informação é caracterizado pela preservação de:

I.que é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

II.que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

III.que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Preencham correta e respectivamente as lacunas I, II e III:

(a)disponibilidade – integridade – confidencialidade

(b)confidencialidade – integridade – disponibilidade

(c)integridade – confidencialidade – disponibilidade

(d)confidencialidade – disponibilidade - integridade

(e) disponibilidade - confidencialidade – integridade

90. **(FCC/TRT-24ª Região/Analista Judiciário/Tecnologia da Informação/2011/Adaptada)** Considere:

I. Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

II. Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

III. Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Na ISO/IEC 17799(renomeada para 27002), I, II e III correspondem, respectivamente, a

a) disponibilidade, integridade e confiabilidade.

b) confiabilidade, integridade e distributividade.

c) confidencialidade, integridade e disponibilidade.

d) confidencialidade, confiabilidade e disponibilidade.

e) integridade, confiabilidade e disponibilidade.

91. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Em relação à vulnerabilidades e ataques a sistemas computacionais, é correto afirmar:

a) Medidas de segurança podem ser definidas como ações que visam eliminar riscos para evitar a concretização de uma vulnerabilidade.

b) O vazamento de informação e falha de segurança em um *software* constituem vulnerabilidades.

c) Roubo de informações e perda de negócios constitui ameaças.

d) Medidas de segurança podem ser definidas como ações que visam eliminar vulnerabilidades para evitar a concretização de uma ameaça.

e) Área de armazenamento sem proteção e travamento automático da estação após período de tempo sem uso constituem ameaça.

92. **(FCC/TRE-CE/Analista Judiciário/Análise de Sistemas/2012)** Ao elaborar e comunicar uma Política de Segurança da Informação - PSI é necessário usar uma linguagem conhecida e meios adequados aos tipos de mensagens e usuários; adotar estilo simples e claro; respeitar o interlocutor sem superestimá-lo nem subestimá-lo; respeitar a cultura organizacional e a do país a que se destina. Nesse sentido, é correto concluir que tal afirmação

a) adere parcialmente às expectativas de uma PSI, pois a política deve ser única, e não deve levar em conta características humanas e legais do país no qual ela é aplicada.

b) adere parcialmente às expectativas de uma PSI, tendo em vista que ela deve ser construída considerando uma linguagem tecnológica desvinculada de adoção de estilos.

c) adere integralmente a formulação de uma PSI, pois ao elaborar uma política é necessário que ela seja ajustada a cada instituição e deve ser comunicada de maneira que todos entendam.

d) adere parcialmente às expectativas de uma PSI, porque os atributos do interlocutor não devem constituir relevância, já que todos os usuários, presumivelmente, foram selecionados pela empresa para entenderem a tecnologia usada.

e) não atende aos propósitos de uma PSI, pois linguagem, estilo e interlocutor não podem sobrepor-se à linguagem tecnológica e é preciso levar em conta a cultura do país no qual ela é aplicada, a linguagem tecnológica utilizada e os níveis de sensibilidade de cada tipo de interlocutor.

93. **(FCC/2012/TRT-11ª.Região/Provas de Analista Judiciário e Técnico Judiciário)** Quando o cliente de um banco acessa sua conta corrente através da internet, é comum que tenha que digitar a senha em um teclado virtual, cujas teclas mudam de lugar a cada caractere fornecido. Esse procedimento de segurança visa evitar ataques de

(A) spywares e adwares.

(B) keyloggers e adwares.

(C) screenloggers e adwares.

(D) phishing e pharming.

(E) keyloggers e screenloggers.

94. **(FCC/2011/TRE-TO/Analista Judiciário – Judiciária)** Uma das formas de proteger o sigilo da informação que trafega na Internet é:

a) não fazer os *downloads* em *notebooks*.

b) não responder *e-mails* que chegam "com cópia oculta".

c) mandar *e-mails* somente a pessoas da lista pessoal.

d) não usar a opção "com cópia para" do correio eletrônico.

e) a criptografia

95. **(FCC/2011/TRF - 1.ª Região/Técnico Judiciário – Segurança e Transporte)** Considerando o recebimento de um arquivo executável de fonte desconhecida, no correio eletrônico, a atitude mais adequada diante deste fato é

a) não executá-lo;

b) baixá-lo no seu desktop e executá-lo localmente, somente;

c) repassá-lo para sua lista de endereços solicitando aos mais experientes que o executem;

d) executá-lo diretamente, sem baixá-lo no seu desktop;

e) executá-lo de qualquer forma, porém comunicar o fato ao administrador de sua rede.

96. **(FCC/2009/MPSED/Analista do Ministério Público/Analista de Sistemas)** Consiste em um conjunto de computadores interconectados por meio de uma rede relativamente insegura que utiliza a criptografia e protocolos especiais para fornecer segurança. Esta é uma conceituação básica para:

a) rede privada com comunicação criptográfica simétrica;

b) canal privado de comunicação assimétrica;

c) canal privado de comunicação síncrona;

d) rede privada com autenticação digital;

e) rede privada virtual.

97. **(Elaboração própria)** Trata-se de um software malicioso que, ao infectar um computador, criptografa todo ou parte do conteúdo do disco rígido. Os responsáveis por esse software exigem da vítima um pagamento pelo "resgate" dos dados.

a) bot;

b) DoS;

c) DDoS;

d) pharming;

e) ransomware.

98. **(FCC/2008/TCE-SP/Adaptada)** Em relação a Certificado Digital, é correto afirmar que: [os certificados servem para garantir a segurança dos dados enviados via upload].

99. **(FCC/2008/TCE-SP/Adaptada)** Em relação a Certificado Digital, é correto afirmar que: são *plugins* que definem a qualidade criptográfica das informações que trafegam na WWW.

100. **(FCC/2008/TCE-SP)** *Secure Sockets Layer* trata-se de

a) qualquer tecnologia utilizada para proteger os interesses de proprietários de conteúdo e serviços;

b) um elemento de segurança que controla todas as comunicações que passam de uma rede para outra e, em função do que sejam, permite ou denega a continuidade da transmissão;

c) uma técnica usada para garantir que alguém, ao realizar uma ação em um computador, não possa falsamente negar que realizou aquela ação;

d) uma técnica usada para examinar se a comunicação está entrando ou saindo e, dependendo da sua direção, permiti-la ou não;

e) um protocolo que fornece comunicação segura de dados através de criptografia do dado.

GABARITO

1. Item **errado.**
2. Item **correto.**
3. Item **correto.**
4. Item **correto.**
5. Item **errado.**
6. Item **correto.**
7. Item **correto.**
8. Item **errado.**
9. Item **errado.**
10. Item **correto.**
11. Item **correto.**
12. Item **errado.**
13. Item **correto.**
14. Item **errado.**
15. Item **errado.**
16. Item **errado.**
17. Item **errado.**
18. Item **correto.**
19. Item **errado.**
20. Item **errado.**
21. Item **errado.**
22. Item **correto.**
23. Item **errado.**
24. Item **errado.**
25. Item **errado.**
26. Item **correto.**
27. Item **errado.**
28. Item **errado.**
29. Item **errado.**
30. Item **correto.**
31. Item **errado.**
32. Item **errado.**
33. Item **errado.**
34. Item **errado.**
35. Item **errado.**
36. Item **errado.**
37. Item **correto.**
38. Item **errado.**
39. Item **errado.**
40. Item **errado.**
41. Item **errado.**
42. Item **errado.**
43. Item **errado.**
44. Item **correto.**
45. Item **errado.**
46. Item **correto.**
47. Item **correto.**
48. Item **correto.**
49. Item **errado.**
50. Item **errado.**
51. Item **errado.**
52. Item **errado.**
53. Item **errado.**
54. Item **correto.**
55. Item **errado.**
56. Item **errado.**
57. Item **errado.**
58. Item **errado.**
59. Item **correto.**
60. Item **errado.**
61. Item **errado.**
62. Item **errado.**
63. Item **errado.**
64. Item **correto.**
65. Item **correto.**
66. Item **anulado**.

67. Item **correto.**
68. Item **correto.**
69. Item **errado.**
70. Item **errado.**
71. Item **correto.**
72. Item **correto.**
73. Item **errado.**
74. Item **errado.**
75. Item **errado.**
76. Item **errado.**
77. Item **correto.**
78. Item **errado.**
79. Item **errado.**
80. Item **errado.**
81. Item **errado.**
82. Item **correto.**
83. Item **errado.**
84. Item **errado.**
85. Item **errado.**
86. Item **errado.**
87. Letra **B.**
88. Letra **A.**
89. Letra **B.**
90. Letra **C.**
91. Letra **D.**
92. Letra **C.**
93. Letra **E.**
94. Letra **E.**
95. Letra **A.**
96. Letra **E.**
97. Letra **E.**
98. Item **errado**.
99. Item **errado**.
100. Letra **E.**

ACOMPANHE A EVOLUÇÃO DO SEU APROVEITAMENTO

Data	Nº questões	Acertos	% acerto	Data	Nº questões	Acertos	% acerto
	100				100		
Data	**Nº questões**	**Acertos**	**% acerto**	**Data**	**Nº questões**	**Acertos**	**% acerto**
	100				100		
Data	**Nº questões**	**Acertos**	**% acerto**	**Data**	**Nº questões**	**Acertos**	**% acerto**
	100				100		
Data	**Nº questões**	**Acertos**	**% acerto**	**Data**	**Nº questões**	**Acertos**	**% acerto**
	100				100		
Data	**Nº questões**	**Acertos**	**% acerto**	**Data**	**Nº questões**	**Acertos**	**% acerto**
	100				100		